

# **Οδηγός Διαχείρισης – Λειτουργίας Σχολικού Εργαστηρίου Windows 2000 Server**

***ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:***

***Τεχνικοί ΚΕΠΛΗΝΕΤ  
Πανεπιστημίου Μακεδονίας***

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ**

**ΤΜΗΜΑ ΠΑΝΕΛΛΗΝΙΟΥ ΣΧΟΛΙΚΟΥ ΔΙΚΤΥΟΥ**



## ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΔΙΚΤΥΩΣΗΣ .....	3
Εισαγωγή στο TCP/IP .....	3
Networking Interfaces .....	3
Διευθύνσεις IP .....	3
Δημόσιες IP διευθύνσεις και ιδιωτικές .....	4
Address Resolution .....	5
IP Routing .....	5
Δίκτυα IP .....	5
Subnetworks .....	6
Gateways .....	6
Γενικές αρχές δικτύωσης σχολικών εργαστηρίων .....	8
ΚΑΡΤΕΛΑ TCP/IP ΣΤΑ WINDOWS 2000 SERVER .....	9
ΔΟΜΗ ΣΧΟΛΙΚΟΥ ΕΡΓΑΣΤΗΡΙΟΥ .....	12
ΓΕΝΙΚΗ ΤΟΠΟΛΟΓΙΑ ΤΟΥ ΣΧΟΛΙΚΟΥ ΔΙΚΤΥΟΥ .....	13
Φυσική Διασύνδεση Ενεργού Εξοπλισμού .....	14
Τύποι δικτύων .....	16
Δίκτυα Peer-to-Peer .....	16
Δίκτυα Client-Server .....	16
Υλοποίηση της δικτύωσης στα Windows 2000 .....	17
Τα στοιχεία ενός Domain .....	17
Οργάνωση του Domain .....	18
TROUBLESHOOTING .....	20
DNS .....	21
Ο ρόλος του DNS Server .....	21
Ρυθμίζοντας – Παραμετροποιώντας τον server .....	21
Windows2000 Server - Εγκατάσταση και ρυθμίσεις υπηρεσίας DNS- Αναλυτικές οδηγίες .....	22
Εγκατάσταση της υπηρεσίας DNS .....	22
Ρυθμίσεις της υπηρεσίας DNS .....	25
Ορισμός Forwarders .....	26
Ορισμός Forward Lookup Zone .....	28
Reverse Lookup Zones .....	33
Troubleshooting .....	40
DHCP .....	41
ρόλος του DHCP Server .....	41
Troubleshooting .....	41
Τοπικοί χρήστες - ομάδες .....	42
Local – Domain user (τοπικός χρήστης- χρήστης τομέα) .....	42
Δημιουργία –διαχείριση τοπικών χρηστών και ομάδων .....	42
Active Directory .....	46
1. Active Directory Directory Service .....	46
2. Active Directory Objects .....	46
3. User Accounts .....	48
4. Groups .....	55
Troubleshooting .....	59
Organization Unit's .....	61
Τί είναι το OU(organizational unit); .....	61



Γιατί να χρησιμοποιούμε ΟΥ; .....	61
Πώς μπορούμε να δημιουργήσουμε ένα ΟΥ; .....	62
Πώς μπορούμε να αλλάξουμε τα χαρακτηριστικά ενός ΟΥ; .....	63
Κοινή Χρήση Φακέλων (Shared Folders) .....	67
Χρήση Κοινόχρηστων Φακέλων .....	67
Προαπαιτούμενα για Κοινή Χρήση .....	68
Μοιράζοντας έναν Φάκελο .....	68
Προσωρινή αποθήκευση (Caching) – Offline Files .....	70
Δικαιώματα Κοινόχρηστων Φακέλων .....	71
Εκχώρηση δικαιωμάτων Κοινόχρηστου Φακέλου.....	74
Τροποποίηση ρυθμίσεων Κοινόχρηστου Φακέλου .....	75
Κοινόχρηστοι Φάκελοι Διαχείρισης.....	76
Ασφάλεια .....	77
Δικαιώματα NTFS.....	77
Πολλαπλά Δικαιώματα NTFS .....	78
Μεταβίβαση δικαιωμάτων NTFS .....	80
Αντιγραφή και Μετακίνηση Αρχείων και Φακέλων .....	81
Εφαρμογή δικαιωμάτων NTFS .....	82
Εκχώρηση δικαιωμάτων NTFS.....	83
Ρύθμιση Μεταβίβασης Δικαιωμάτων .....	85
Συνιστώμενες Πρακτικές.....	86
Συνδυασμός δικαιωμάτων NTFS και Κοινής Χρήσης.....	87



## ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΔΙΚΤΥΩΣΗΣ

### Εισαγωγή στο TCP/IP

Όπως και όλα τα άλλα πρωτόκολλα επικοινωνιών, το TCP/IP αποτελείται από επίπεδα:

**IP** - είναι υπεύθυνο για την διακίνηση πακέτων δεδομένων από κόμβο σε κόμβο. Το IP προωθεί κάθε πακέτο με βάση μία διεύθυνση προορισμού τεσσάρων bytes (αριθμός IP). Οι αρχές του Internet αναθέτουν εύρος αριθμών σε διάφορους οργανισμούς. Οι οργανισμοί αναθέτουν ομάδες των δικών τους αριθμών στα τμήματα. Το IP ενεργεί σε μηχανήματα πύλες (gateways) που μεταφέρουν δεδομένα από το τμήμα στον οργανισμό στην περιφέρεια και τελικά σε όλο τον κόσμο.

**TCP** - είναι υπεύθυνο για την επαλήθευση της σωστής μεταφοράς δεδομένων από τον client στον server. Τα δεδομένα μπορεί να χαθούν στο ενδιάμεσο δίκτυο. Το TCP προσθέτει υποστήριξη στην ανίχνευση λαθών ή χαμένων δεδομένων και στην πρόκληση της επανεκπομπής έως ότου τα δεδομένα ληφθούν σωστά και ολοκληρωμένα.

**Sockets** - είναι η ονομασία ενός πακέτου υπορουτινών οι οποίες προσφέρουν πρόσβαση στο TCP/IP στα περισσότερα συστήματα.

### Networking Interfaces

Για να μην είναι φανερή η ποικιλία του εξοπλισμού που μπορεί να χρησιμοποιεί ένα περιβάλλον δικτύου, το TCP/IP, ορίζει μία αφαιρετική διασύνδεση μέσω της οποίας γίνεται προσβάσιμο το hardware. Αυτή η διασύνδεση προσφέρει μία σειρά από λειτουργίες που είναι ίδιες για όλους τους τύπους του υλικού και βασικά ασχολείται με αποστολή και λήψη πακέτων.

Για κάθε περιφερειακή συσκευή που θέλετε να χρησιμοποιήσετε στο δίκτυο, μία αντίστοιχη διασύνδεση πρέπει να υπάρχει στον πυρήνα. Για παράδειγμα, στο Linux οι διασυνδέσεις Ethernet καλούνται eth0 και eth1, οι διασυνδέσεις SLIP sl0, sl1, κ.λ.π. Στα Windows έχουμε ανάλογα «Σύνδεση τοπικού δικτύου 1», «Σύνδεση τοπικού δικτύου 2». Αυτές οι ονομασίες των διασυνδέσεων χρησιμοποιούνται για να γίνονται οι ρυθμίσεις, όταν θέλουμε να δώσουμε το όνομα μιας συγκεκριμένης συσκευής στον πυρήνα. Δεν έχουν καμιά σημασία πέρα από αυτό.

Για να είναι χρησιμοποιήσιμη για την δικτύωση TCP/IP, μία διασύνδεση πρέπει να έχει κάποια διεύθυνση IP η οποία θα έχει τον ρόλο της ταυτότητας στην επικοινωνία με τον υπόλοιπο κόσμο. Αυτή η διεύθυνση είναι διαφορετική από το όνομα της διασύνδεσης που αναφέρθηκε παραπάνω. Αν συγκρίνουμε μία διασύνδεση με μία πόρτα, τότε η διεύθυνση είναι το ταμπελάκι με το όνομα που είναι κολλημένο σ' αυτήν.

### Διευθύνσεις IP

Οι διευθύνσεις που είναι κατανοητές από το πρωτόκολλο IP, είναι αριθμοί 32 bit. Σε κάθε μηχανήμα πρέπει να ανατίθεται ένας αριθμός μοναδικός στο δικτυακό περιβάλλον. Όταν έχετε ένα τοπικό δίκτυο που δεν έχει κυκλοφορία TCP/IP με άλλα δίκτυα, μπορείτε να αναθέσετε αυτούς τους αριθμούς σύμφωνα με τις προσωπικές σας προτιμήσεις. Όμως, για τις τοποθεσίες στο Internet, οι αριθμοί ανατίθενται από κεντρικές αρχές.



Για πιο εύκολη ανάγνωση, οι διευθύνσεις IP χωρίζονται σε τέσσερις αριθμούς των 8 bit. Για παράδειγμα, όταν ένας υπολογιστής έχει την IP διεύθυνση 0x954C0C04, αυτή γράφεται 149.76.12.4. Ένας άλλος λόγος για αυτόν τον τρόπο γραφής είναι ότι οι διευθύνσεις IP χωρίζονται σε αριθμό *δικτύου*, που περιέχεται στα τμήματα που προηγούνται, και σε αριθμό *κόμβου*, που είναι τα υπόλοιπα τμήματα.

Για να εξυπηρετηθούν διαφορετικές ανάγκες, υπάρχουν αρκετές κλάσεις δικτύων, ορίζοντας διαφορετικούς διαχωρισμούς του διευθύνσεων IP.

**Class A** 1.0.0.0 ως 127.0.0.0. Ο αριθμός δικτύου περιέχεται στο πρώτο τμήμα. Αυτό παρέχει ένα τμήμα κόμβου των 24 bit, επιτρέποντας περίπου 1.6 εκατομμύρια κόμβους.

**Class B** 128.0.0.0 ως 191.255.0.0. Ο αριθμός δικτύου είναι στα δύο πρώτα τμήματα. Αυτό επιτρέπει 16320 δίκτυα με 65024 κόμβους το καθένα.

**Class C** 192.0.0.0 ως 223.255.255.0. Ο αριθμός δικτύου περιέχεται στα τρία πρώτα τμήματα. Αυτό μας δίνει περίπου 2 εκατομμύρια δίκτυα με έως 254 κόμβους.

Οι κλάσεις D, E, και F που έχουν διευθύνσεις στο εύρος 224.0.0.0 ως 254.0.0.0 είναι είτε πειραματικές ή για μελλοντική χρήση και δεν καθορίζουν κανένα δίκτυο.

Η διεύθυνση 149.76.12.4, σύμφωνα με τα παραπάνω, αναφέρεται στον κόμβο 12.4 στο δίκτυο της κλάσης B 149.76.0.0.

Θα παρατηρήσατε ότι στην παραπάνω λίστα δεν περιλαμβάνονται όλες οι δυνατές τιμές για κάθε τμήμα στην πλευρά του αριθμού του κόμβου. Αυτό γίνεται επειδή αριθμοί κόμβων με τμήματα όλα 0 ή 255 είναι δεσμευμένα για ειδικούς σκοπούς. Μία διεύθυνση όπου όλα τα bit του κόμβου είναι μηδενικά αναφέρεται στο δίκτυο, και μία όπου όλα τα bit του κόμβου είναι 1 καλείται broadcast address. Αυτή αναφέρεται σε όλους τους κόμβους του δικτύου ταυτόχρονα. Έτσι η 149.76.255.255 δεν είναι έγκυρη διεύθυνση κόμβου αλλά αναφέρεται σε όλους τους κόμβους στο δίκτυο 149.76.0.0.

Υπάρχουν επίσης δύο διευθύνσεις δικτύου που είναι δεσμευμένες, 0.0.0.0 και 127.0.0.0. Η πρώτη καλείται *default route*, η δεύτερη *loopback address*. Το δίκτυο 127.0.0.0 δεσμεύεται για την κίνηση IP τοπικά στον κόμβο. Συνήθως, η διεύθυνση 127.0.0.1 θα ανατεθεί σε μία ειδική διασύνδεση στον κόμβο, που ονομάζεται *loopback interface*, η οποία ενεργεί ως κλειστό κύκλωμα. Κάθε πακέτο IP που στέλνεται σ' αυτή από τα TCP ή UDP θα επιστραφεί σ' αυτά σαν να είχαν έρθει από κάποιο δίκτυο. Αυτό σας επιτρέπει να αναπτύσσετε και να ελέγχετε λογισμικό δικτύου χωρίς ποτέ να χρησιμοποιείτε «πραγματικό» δίκτυο.

## Δημόσιες IP διευθύνσεις και ιδιωτικές

Η υπηρεσία Internet Assigned Numbers Authority (IANA) έχει δεσμεύσει τις παρακάτω τρεις ομάδες εύρους IP διευθύνσεων για ιδιωτικά Internet (τοπικά δίκτυα) :

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255



Επίσης, οι διευθύνσεις IP στο εύρος 169.254.0.0 -169.254.255.255 είναι δεσμευμένες για το την Αυτόματη Διευθυνσιοδότηση Ιδιωτικών IP (Automatic Private IP Addressing). Αν έχουμε ένα δίκτυο οι κόμβοι του οποίου είναι ρυθμισμένοι να παίρνουν δυναμικές διευθύνσεις IP και δεν υπάρχει DHCP server στο δίκτυο τότε θα αποδοθούν σ' αυτούς διευθύνσεις από το παραπάνω εύρος.

Όλες οι παραπάνω κατηγορίες διευθύνσεων ονομάζονται ιδιωτικές διευθύνσεις, δεν είναι «ορατές» από το Internet και δεν πρέπει να χρησιμοποιούνται στο Internet.

## Address Resolution

Τώρα που είδατε πως γίνονται οι διευθύνσεις IP, μπορεί να αναρωτιέστε πως χρησιμοποιούνται στο Ethernet για να διευθυνσιοδοτήσουν διαφορετικούς κόμβους. Στο κάτω-κάτω, το πρωτόκολλο Ethernet αναγνωρίζει τους κόμβους από την MAC address η οποία δεν έχει απολύτως τίποτα κοινό με την διεύθυνση IP, έτσι δεν είναι; Σωστά. Για αυτό χρειάζεται ένας μηχανισμός για να αντιστοιχεί τις διευθύνσεις IP στις διευθύνσεις Ethernet. Αυτό ονομάζεται *Address Resolution Protocol*, ή ARP.

Όταν το ARP θέλει να βρει την διεύθυνση Ethernet που αντιστοιχεί σε μία IP, χρησιμοποιεί ένα στοιχείο του Ethernet γνωστό ως “broadcasting”, όπου ένα πακέτο σ' όλους τους κόμβους του δικτύου ταυτόχρονα. Το αποσπελλόμενο πακέτο από το ARP, περιέχει ένα ερώτημα για την διεύθυνση IP. Κάθε κόμβος που το παραλαμβάνει το συγκρίνει με την δική του IP, και αν ταιριάζει, επιστρέφει μια απάντηση ARP στον ενδιαφερόμενο κόμβο. Ο ενδιαφερόμενος κόμβος τώρα μπορεί να βρει την διεύθυνση Ethernet του αποστολέα από την απάντηση. Αφού ένας κόμβος έχει βρει μια διεύθυνση Ethernet, την αποθηκεύει στη cache του ARP ώστε να μη χρειαστεί να ξαναρωτήσει την επόμενη φορά που θα θέλει να στείλει πακέτα σ' αυτόν τον κόμβο. Όμως δεν είναι σοφό να διατηρείται αυτή η πληροφορία για πάντα, π.χ. η κάρτα Ethernet ενός απομακρυσμένου κόμβου μπορεί να αντικατασταθεί λόγω τεχνικών προβλημάτων, έτσι αυτή η καταχώρηση του ARP γίνεται άκυρη. Για να γίνει αναγκαστικά νέο ερώτημα για IP διευθύνσεις, οι καταχωρήσεις της cache ARP αγνοούνται μετά από κάποιο χρονικό διάστημα.

## IP Routing

### Δίκτυα IP

Όταν γράφετε ένα γράμμα σε κάποιον, συνήθως γράφετε μια πλήρη διεύθυνση στον φάκελο, προσδιορίζοντας την χώρα, την πόλη, τον ταχυδρομικό κωδικό, κ.α. Αφού το ρίξετε στο γραμματοκιβώτιο, η ταχυδρομική υπηρεσία θα το μεταφέρει στον προορισμό του: θα σταλεί στην υποδεικνυόμενη χώρα, της οποίας η αντίστοιχη υπηρεσία θα το προωθήσει στην περιφέρεια, πόλη, κ.λ.π. Το πλεονέκτημα αυτού του ιεραρχικού σχήματος είναι μάλλον προφανές: Όταν ταχυδρομείτε ένα γράμμα, το τοπικό ταχυδρομείο ξέρει μόνο την κατεύθυνση να προωθήσει το γράμμα, αλλά δεν ενδιαφέρεται με ποιο τρόπο θα ταξιδέψει η επιστολή μέσα στην χώρα προορισμού. Τα δίκτυα IP είναι δομημένα με ανάλογο τρόπο. Ολόκληρο το Internet αποτελείται από έναν αριθμό κατάλληλων δικτύων, που καλούνται *αυτόνομα συστήματα*. Κάθε τέτοιο σύστημα εκτελεί κάθε είδους δρομολόγηση ανάμεσα στους κόμβους που είναι μέλη του εσωτερικά, ούτως ώστε η εργασία της διανομής ενός πακέτου μειώνεται στην εύρεση της διαδρομής προς το δίκτυο του κόμβου προορισμού. Αυτό σημαίνει, ότι μόλις το πακέτο παραδοθεί σε οποιονδήποτε κόμβο που είναι σ' αυτό το





συγκεκριμένο δίκτυο, η περαιτέρω επεξεργασία γίνεται αποκλειστικά από το ίδιο το δίκτυο.

## Subnetworks

Αυτή η δομή δημιουργείται διαιρώντας τις διευθύνσεις IP σε μέρος δικτύου και κόμβου, όπως εξηγήθηκε παραπάνω. Εξ ορισμού, το δίκτυο προορισμού αποτελείται από το τμήμα δικτύου της διεύθυνσης IP. Έτσι, κόμβοι με ταυτόσημους αριθμούς δικτύου θα πρέπει να βρίσκονται στο ίδιο δίκτυο και αντίστροφα.

Έχει νόημα να δημιουργήσουμε ένα παρόμοιο σχήμα μέσα στο δίκτυο επίσης, αφού μπορεί να αποτελείται από συλλογή εκατοντάδων δικτύων, με τις μικρότερες μονάδες να είναι φυσικά δίκτυα σαν τα Ethernet. Γι' αυτό το IP μας επιτρέπει να υποδιαιρέσουμε ένα δίκτυο IP σε αρκετά υποδίκτυα.

Ένα υποδίκτυο αναλαμβάνει την ευθύνη της διανομής πακέτων σε ένα ορισμένο εύρος διευθύνσεων IP από το δίκτυο IP του οποίου είναι μέρος. Όπως με τις κλάσεις A, B, C, αναγνωρίζεται από το τμήμα διευθύνσεων της διεύθυνσης IP. Παρ' όλα αυτά, το τμήμα δικτύου τώρα επεκτείνεται για να συμπεριλάβει κάποια bit από το τμήμα κόμβου. Ο αριθμός των bit τα οποία διερμηνεύονται ως αριθμός υποδικτύου δίδεται από την επονομαζόμενη μάσκα υποδικτύου (*subnet mask*, ή *netmask*). Αυτός είναι επίσης ένας αριθμός 32 bit ο οποίος καθορίζει την μάσκα των bit για το τμήμα δικτύου της διεύθυνσης IP.

Αξίζει να σημειώσουμε ότι το *sub-netting* (έτσι ονομάζεται η τεχνική δημιουργίας υποδικτύων) είναι *εσωτερική* μόνο διαίρεση του δικτύου. Τα υποδίκτυα δημιουργούνται από τους διαχειριστές των δικτύων και συχνά αντανakλούν διάφορα «σύνορα», έστω φυσικά (μεταξύ δύο Ethernet), διαχειριστικά (μεταξύ δύο τμημάτων) ή γεωγραφικά. Όπως είπαμε πάντως, αυτή η δομή επηρεάζει μόνο την εσωτερική συμπεριφορά του δικτύου, και είναι τελείως αόρατη στον έξω κόσμο.

Ο συνδυασμός του δικτύου με το υποδίκτυο μαζί γράφεται είτε παραθέτοντας το δίκτυο και την μάσκα υποδικτύου π.χ. *192.168.0.0/255.255.255.0* είτε παραθέτοντας το δίκτυο και τον αριθμό των bit της μάσκας υποδικτύου που ισούνται με 1, π.χ. το παραπάνω παράδειγμα μπορεί να γραφτεί και ως *192.168.0.0/24*.

## Gateways

Η δημιουργία υποδικτύων δεν είναι μόνο ένα οργανωτικό πλεονέκτημα, είναι συχνά μία φυσική επίπτωση ορίων hardware. Η εμβέλεια ενός κόμβου σε ένα δοσμένο φυσικό δίκτυο, όπως ένα Ethernet, είναι πολύ περιορισμένη: οι μόνοι κόμβοι στους οποίους μπορεί να μιλήσει απευθείας είναι αυτοί του δικτύου στο οποίο είναι συνδεδεμένος. Όλοι οι άλλοι κόμβοι μπορεί να είναι προσβάσιμοι μόνο μέσω αυτών που αποκαλούνται πύλες (*gateways*). Η πύλη είναι ένας κόμβος ο οποίος είναι συνδεδεμένος σε δύο ή περισσότερα φυσικά δίκτυα ταυτόχρονα και είναι ρυθμισμένος να ανταλλάσσει πακέτα μεταξύ τους.

Έτσι, σε μία πύλη μία διεύθυνση IP για κάθε δίκτυο στο οποίο ανήκει. Αυτές οι διευθύνσεις - μαζί με τις αντίστοιχες *netmask* - ορίζονται στην διασύνδεση με την οποία είναι προσβάσιμο το υποδίκτυο. Έτσι για ένα κόμβο που είναι πύλη και συνδέεται στα δίκτυα 149.76.4.0 και 149.76.1.4, μία αντιστοίχιση διασυνδέσεων και διευθύνσεων θα μπορούσε να είναι ως εξής:



```
-----  
+-----+-----+-----+  
|iface | address | netmask |  
+-----+-----+-----+  
|eth0 | 149.76.4.1 | 255.255.255.0 |  
|fddi0 | 149.76.1.4 | 255.255.255.0 |  
|lo | 127.0.0.1 | 255.0.0.0 |  
+-----+-----+-----+  
+-----+-----+-----+
```





## Γενικές αρχές δικτύωσης σχολικών εργαστηρίων

- Σε κάθε σχολική μονάδα αποδίδεται ένα private IP υποδίκτυο της μορφής [10.x.y.0/24]. Ο εξυπηρετητής (server) του εργαστηρίου θα πρέπει να έχει static IP της μορφής 10.x.y.10. Εάν υπάρχει ήδη εξυπηρετητής στο σχολείο με αυτή την IP, στο νέο server θα αποδοθεί η IP διεύθυνση 10.χ.γ.11.
- Ο εξυπηρετητής του σχολείου (όταν πάρει την IP διεύθυνση 10.x.y.10) είναι δυνατό να είναι ορατός από το Internet με την διεύθυνση: srv-<full dns name σχολείου>.
- Υπηρεσία DHCP θα δίνει ο δρομολογητής του σχολείου και όχι ο εξυπηρετητής του εργαστηρίου. Οι σταθμοί εργασίας του εργαστηρίου θα ρωτάνε για DNS πρώτα τον εξυπηρετητή του εργαστηρίου και εάν αυτός δεν απαντά θα ρωτάνε απευθείας τους εξωτερικούς DNS Servers του EDUnet.
- Υπηρεσία DHCP θα δίνει ο δρομολογητής του εργαστηρίου ο οποίος θα μοιράζει scope διευθύνσεων 10.x.y.128-10.x.y.254
- Οι διευθύνσεις στην περιοχή 10.x.y.16-10.x.y.127 μπορούν να χρησιμοποιηθούν για στατική απόδοση σε σταθμούς εργασίας, servers, και δικτυακές συσκευές οι οποίες έχουν πρόσβαση στο Internet μέσω NAT/PAT (NAT overload).
- Οι ιδιωτικές διευθύνσεις αντιστοιχίζονται σε πραγματικές ip διευθύνσεις μέσω λειτουργίας NAT που πραγματοποιείται στον δρομολογητή του δικτύου πρόσβασης.

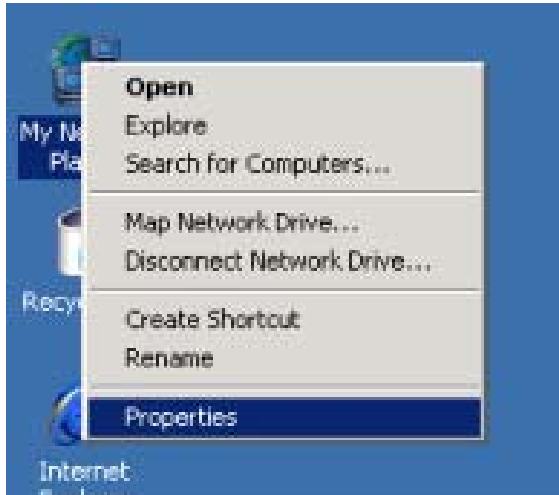


## ΚΑΡΤΕΛΑ TCP/IP ΣΤΑ WINDOWS 2000 SERVER

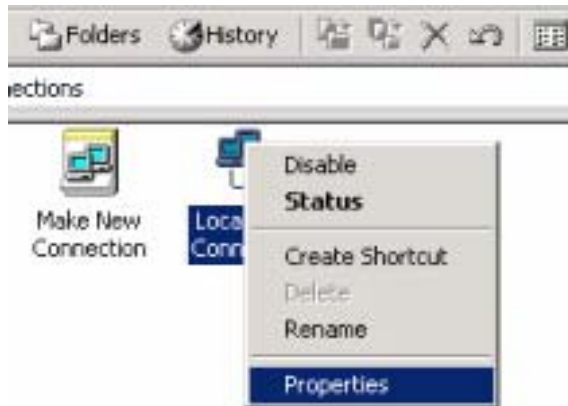
Ο server στο σχολικό εργαστήριο έχει διεύθυνση της μορφής 10.X.Y.10 ενώ ο router 10.X.Y.1. Επίσης ο router είναι και η πύλη του εργαστηρίου (default gateway).

Ας δούμε τώρα πως ρυθμίζουμε το TCP/IP σε έναν server με Windows 2000.

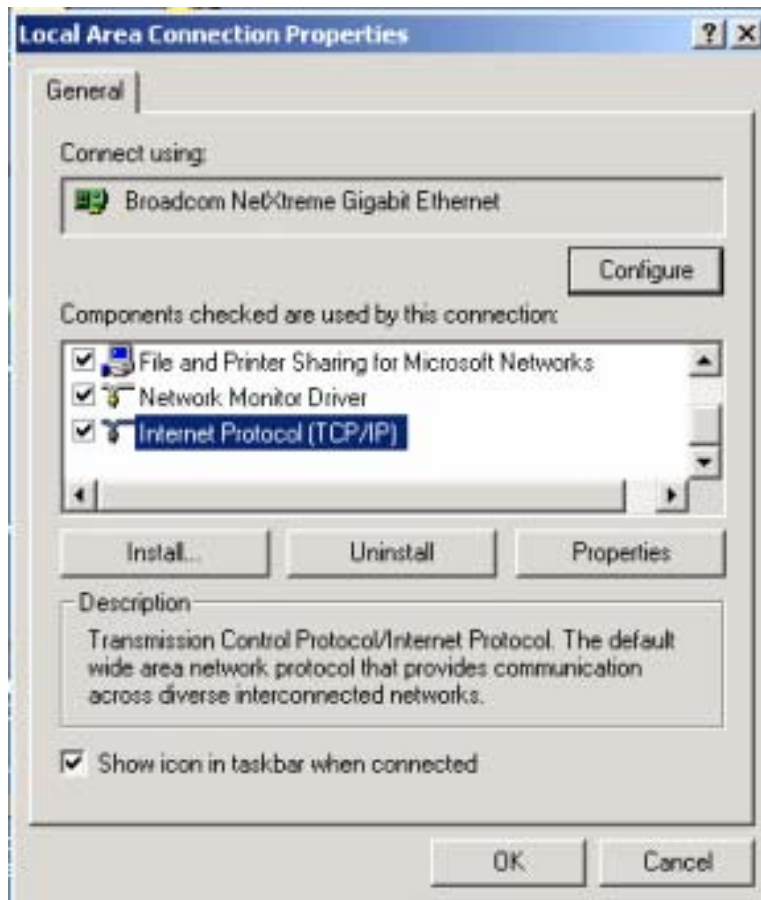
Μετά από δεξί κλικ στο εικονίδιο “My Network Places” επιλέγουμε το “Properties”.



Κάνουμε δεξί κλικ στο εικονίδιο του τοπικού δικτύου και επιλέγουμε “Properties”



Στη συνέχεια επιλέγουμε το “Internet Protocol (TCP/IP)” από την λίστα των πρωτοκόλλων και υπηρεσιών που είναι εγκατεστημένα στον server και πατάμε το κουμπί “Properties”.



Εμφανίζεται η καρτέλα όπου δίνουμε τις κύριες πληροφορίες για την ρύθμιση του TCP/IP. Τσεκάρουμε την επιλογή “Use the following IP address”. Στο πεδίο “IP address” γράφουμε την IP διεύθυνση του server (είναι της μορφής 10.X.Y.10). Στο πεδίο “Subnet mask” γράφουμε την μάσκα υποδικτύου που είναι σε όλους του servers ίδια, 255.255.255.0. (Ποιο είναι το τμήμα δικτύου και ποιο το τμήμα κόμβου της διεύθυνσης του server;). Ως default gateway ή προεπιλεγμένη πύλη είπαμε ότι χρησιμοποιούμε τον router, επομένως στο πεδίο “Default gateway” γράφουμε την IP του router που είναι της μορφής 10.X.Y.1.



Στο τμήμα των DNS servers γράφουμε τις IP των DNS servers που χρησιμοποιούμε για την επίλυση των ονομάτων. Ως “Preferred DNS server” ορίζουμε τον server του σχολικού εργαστηρίου που εκτελεί υπηρεσίες DNS (συνήθως ο ίδιος ο server). Ως “Alternate DNS server” δεν ορίζουμε κανένα. Η υπηρεσία DNS του server αναλαμβάνει την προώθηση των αιτημάτων προς τους εξωτερικούς DNS servers του EDUNET.

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address: 10 . 132 . 18 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 132 . 18 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 10 . 132 . 18 . 10

Alternate DNS server: . . .

Advanced...

OK Cancel



## ΔΟΜΗ ΣΧΟΛΙΚΟΥ ΕΡΓΑΣΤΗΡΙΟΥ

Κάθε σχολικό εργαστήριο σχηματίζεται από μια συλλογή ηλεκτρονικών υπολογιστών συνδεδεμένων σε ένα τοπικό δίκτυο που ακολουθούν την αρχιτεκτονική πελάτη-εξυπηρετητή. Ο εξυπηρετητής λειτουργεί σε περιβάλλον Windows 2000 Server και αναλαμβάνει την υλοποίηση του μεγαλύτερου τμήματος της λειτουργικότητας του εργαστηρίου σε ότι αφορά τις προσφερόμενες υπηρεσίες και την εφαρμογή της πολιτικής που θα ικανοποιεί τα προαναφερόμενα κριτήρια.

Οι σταθμοί εργασίας λειτουργούν σε περιβάλλον ελληνικών Windows 2000 Professional και είναι αυστηρά προσαρμοσμένοι στη συμμετοχή τους σε μια περιοχή (Windows domain) σχηματισμένη από τον εξυπηρετητή (είναι δυνατή η χρήση Windows XP Home & Professional ή οποιασδήποτε μεταγενέστερης έκδοσης λειτουργικού συστήματος της Microsoft για σταθμούς εργασίας είναι σε θέση να ενσωματωθεί σωστά σε ένα περιβάλλον Windows 2000 Server). Είναι εγκατεστημένοι και ρυθμισμένοι κατάλληλα ώστε κάθε παράμετρος της λειτουργίας τους να εξαρτάται άμεσα από τις σχετικές ρυθμίσεις στα Windows 2000 Server, ενώ η ανεξάρτητη από την περιοχή χρήση τους είναι ουσιαστικά αδύνατη.

Ένας σταθμός εργασίας σε κάθε σχολικό εργαστήριο μπορεί να είναι εγκατεστημένος σε κατάσταση διπλής εκκίνησης (dual-boot), όπου το δεύτερο λειτουργικό σύστημα είναι το Linux, για την υποστήριξη επιπλέον υπηρεσιών σε όλο το εργαστήριο, οπότε και ο συγκεκριμένος σταθμός εργασίας λειτουργεί ως διακομιστής. Το σύστημα Linux συνεργάζεται με τον Windows 2000 Server για την πιστοποίηση των χρηστών και προσφέρει υπηρεσίες όπως διαμοίραση αρχείων, εκτύπωση, ηλεκτρονικό ταχυδρομείο (view και caching).

Το τοπικό δίκτυο υλοποιείται με την εγκατάσταση των απαραίτητων δικτυακών συσκευών, ενώ γίνεται χρήση μόνο του πρωτοκόλλου IP για την επικοινωνία των σταθμών εργασίας τόσο μεταξύ τους όσο και με τον εξυπηρετητή.

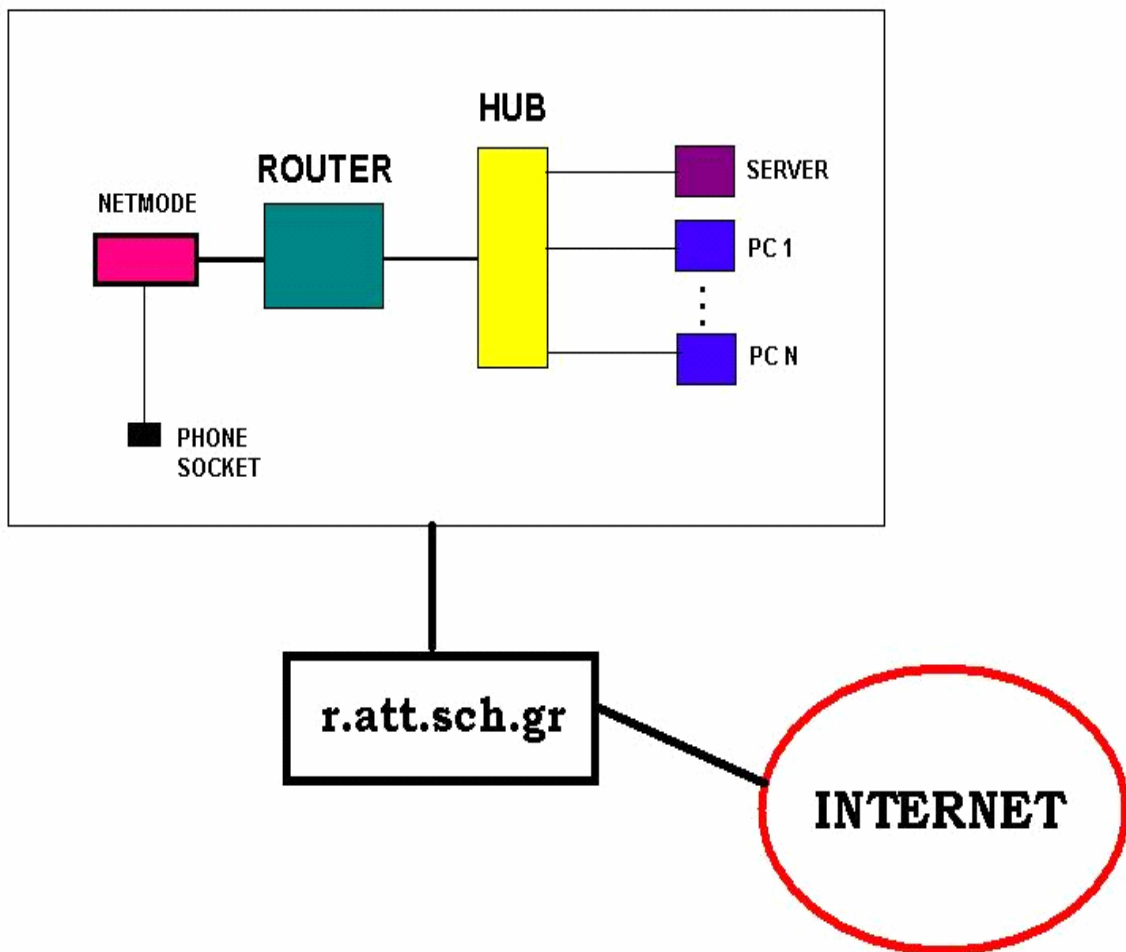
Η δικτυακή επικοινωνία του σχολικού εργαστηρίου με το διαδίκτυο πραγματοποιείται με ποικιλία διαφορετικών τρόπων (αναλογικές μισθωμένες γραμμές, ISDN dial-up, ασύρματες ή άλλες συνδέσεις) με χρήση του απαραίτητου εξοπλισμού ρυθμισμένου με βάση τις προδιαγραφές του Πανελληνίου Σχολικού Δικτύου. Τέλος, οι υπάρχουσες περιφερειακές συσκευές (εκτυπωτής, σαρωτής, κάμερα κλπ) είναι εγκατεστημένες με τέτοιο τρόπο ώστε να γίνεται εκμετάλλευση των δυνατοτήτων του περιβάλλοντος Windows 2000 Server. Όπου είναι δυνατόν οι περιφερειακές συσκευές που δεν έχουν δικτυακό χαρακτήρα είναι εγκατεστημένες στο dual-boot μηχάνημα και παρέχεται η δυνατότητα χρήσης τους από όλα τα υποστηριζόμενα λειτουργικά συστήματα.



## ΓΕΝΙΚΗ ΤΟΠΟΛΟΓΙΑ ΤΟΥ ΣΧΟΛΙΚΟΥ ΔΙΚΤΥΟΥ

Η γενική κατανόηση της τοπολογίας του δικτύου, καθώς και των ρόλων των επιμέρους υπο-σταθμών, είναι καθοριστικό στην διάγνωση των προβλημάτων που δύναται να παρουσιαστούν.

Μία συγκεντρωτική όψη της δομής φαίνεται στο ακόλουθο σχήμα.





## Φυσική Διασύνδεση Ενεργού Εξοπλισμού

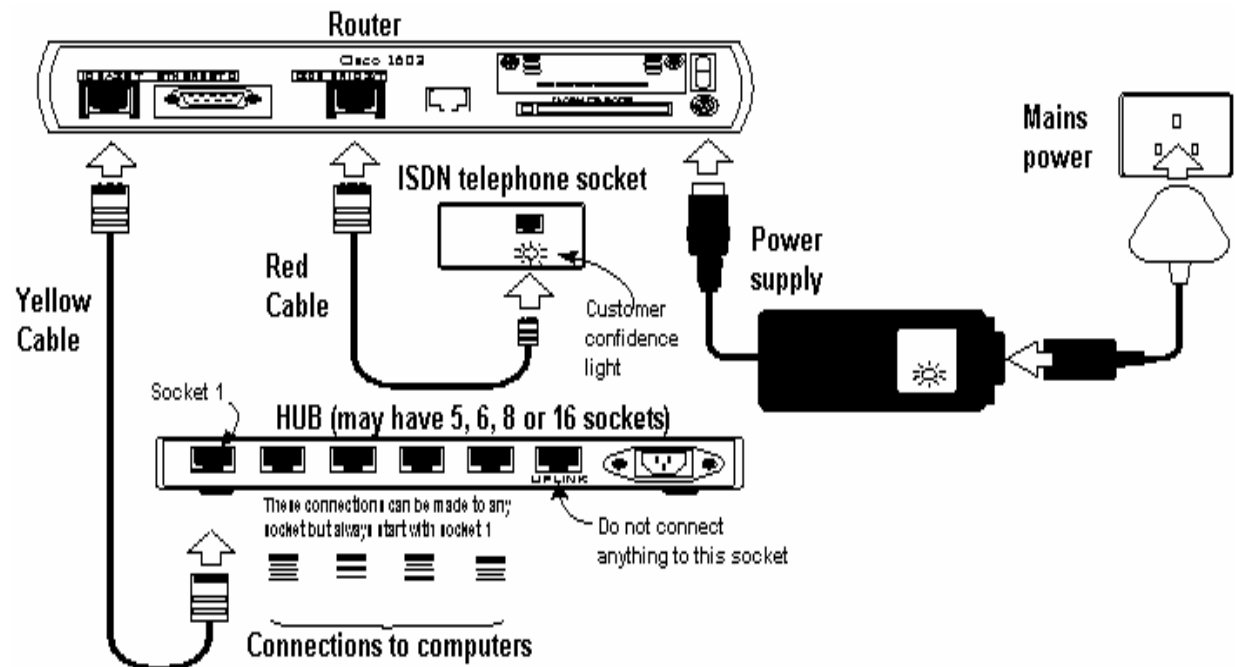
10Base-T

ISDN

Console

Netmod

Power



Η αναλυτική διάρθρωση υλοποιείται κατά τον εξής τρόπο :

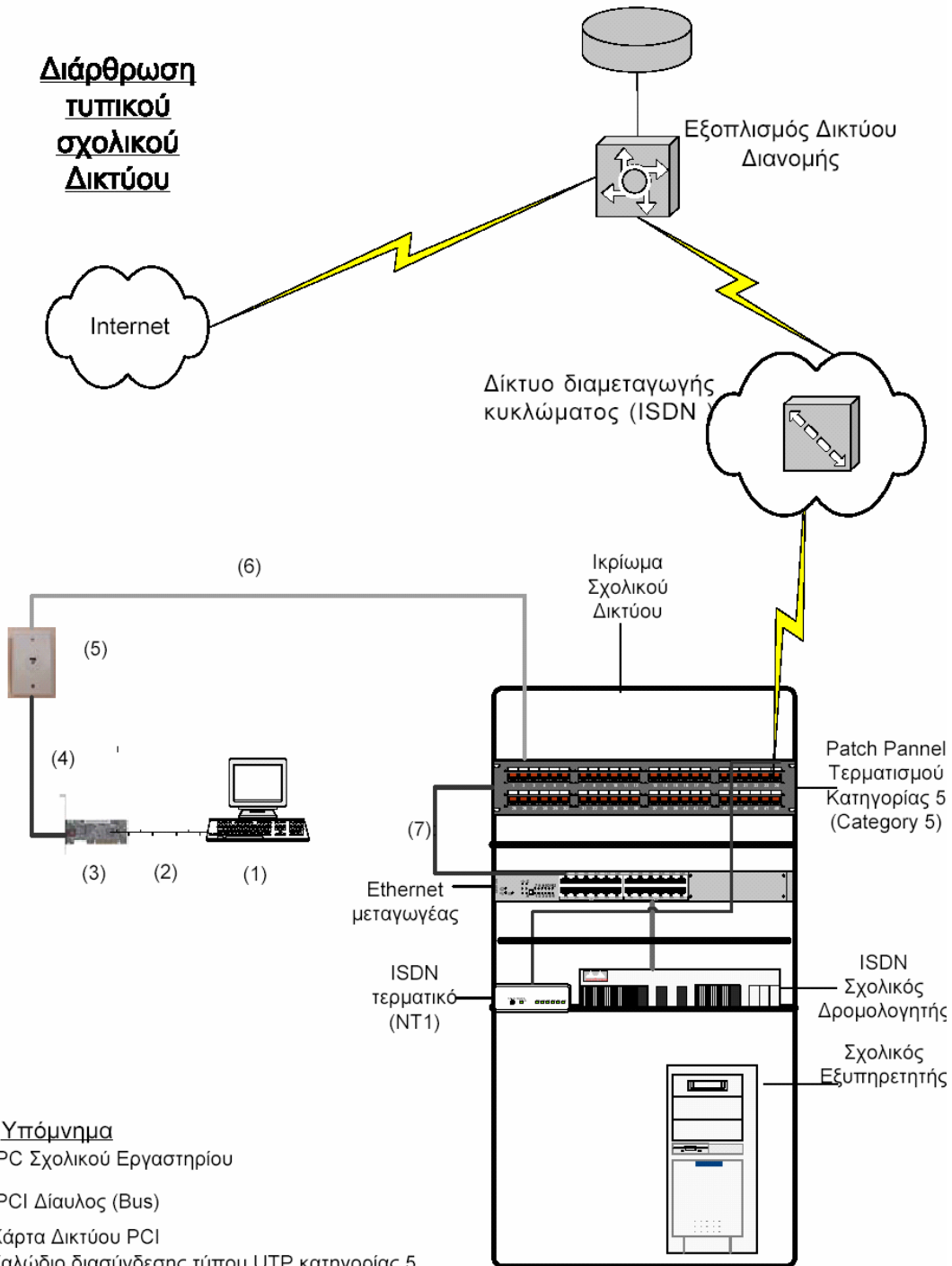
Οι σταθμοί εργασίας (PC) καθώς και ο SERVER συνδέονται στο HUB.

Το HUB συνδέεται στον ROUTER

ROUTER συνδέεται στο κουτί του ISDN (Netmod)

Το NETMOD συνδέεται στην τηλεφωνική γραμμή.



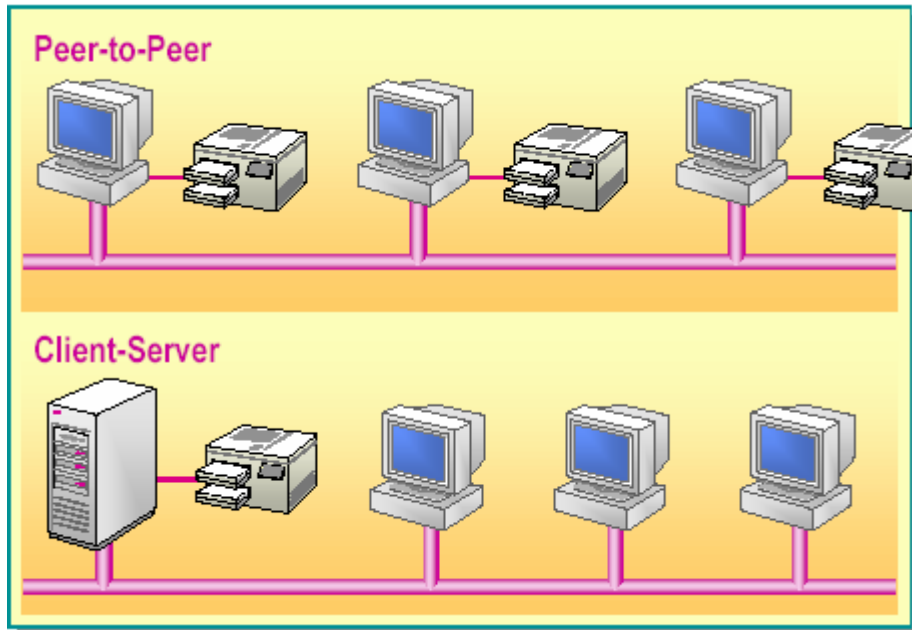


#### Υπόμνημα

- (1): PC Σχολικού Εργαστηρίου
- (2): PCI Δίαυλος (Bus)
- (3):Κάρτα Δικτύου PCI
- (4) Καλώδιο διασύνδεσης τύπου UTP κατηγορίας 5 (Category 5)
- (5) Πρίζα data Κατηγορίας 5 (Category 5)
- (6): ενδοκτιριακό/ενδοκανάλιο καλώδιο UTP 4" κατηγορίας 5 (Category 5)
- (7): jumper patch cord UTP κατηγορίας 5 (Category 5)



## Τύποι Δικτύων



Βασισμένα στο πώς είναι διαμορφωμένοι οι υπολογιστές σε ένα δίκτυο και πώς έχουν πρόσβαση στις πληροφορίες, τα δίκτυα χωρίζονται σε δύο κατηγορίες: peer-to-peer και client-server. Οι διαφορές στις δύο κατηγορίες είναι σημαντικές γιατί κάθε κατηγορία έχει διαφορετικές δυνατότητες.

### Δίκτυα Peer-to-Peer

Σε ένα peer-to-peer δίκτυο, δεν υπάρχουν εξειδικευμένοι servers και δεν υπάρχει ιεραρχία μεταξύ των υπολογιστών. Όλοι οι υπολογιστές είναι ίσοι μεταξύ τους. Κάθε υπολογιστής λειτουργεί μαζί ως client και ως server και συνήθως δεν υπάρχει διαχειριστής υπεύθυνος για την συντήρηση του δικτύου. Η ασφάλεια παρέχεται από την τοπική βάση καταλόγου κάθε υπολογιστή. Ο χρήστης σε κάθε υπολογιστή αποφασίζει ποια δεδομένα στον υπολογιστή του είναι κοινόχρηστα στο δίκτυο. Τα δίκτυα peer-to-peer ονομάζονται συνήθως **workgroups** (ομάδες εργασίας). Ο όρος **workgroup** περιγράφει μία μικρή ομάδα ατόμων, τυπικά 10 ή λιγότερα, που εργάζονται μαζί. Τα δίκτυα peer-to-peer είναι καλή επιλογή για περιβάλλοντα όπου:

- Υπάρχουν 10 ή λιγότεροι χρήστες.
- Οι χρήστες μοιράζονται πόρους και εκτυπωτές, αλλά δεν υπάρχουν εξειδικευμένοι servers.
- Η ασφάλεια δεν είναι πρόβλημα.
- Ο οργανισμός και το δίκτυο θα έχουν περιορισμένη ανάπτυξη στο προβλεπόμενο μέλλον.

### Δίκτυα Client-Server

Καθώς ένα δίκτυο αναπτύσσεται, ένα δίκτυο peer-to-peer πιθανώς δεν θα μπορεί πλέον να αντεπεξέλθει στις αυξημένες απαιτήσεις για κοινόχρηστους πόρους. Για να



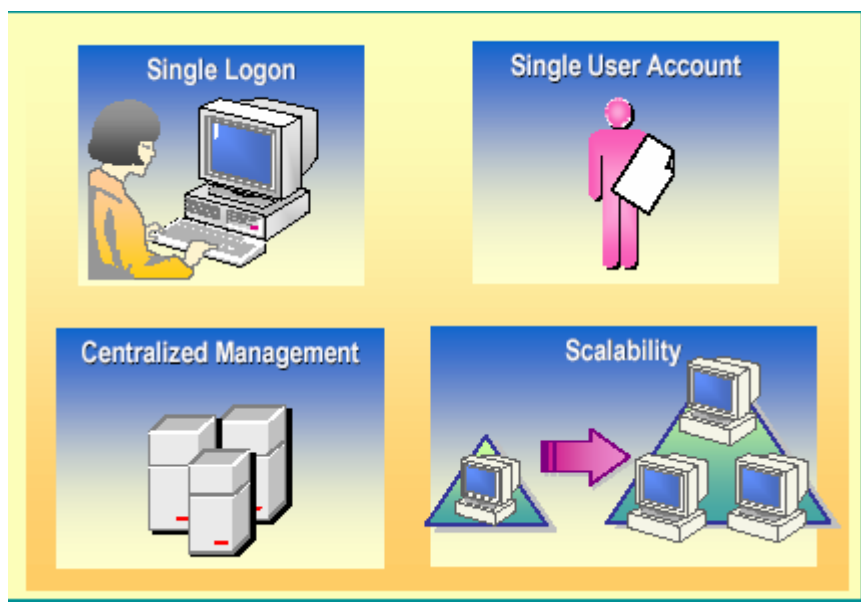
ικανοποιηθούν οι αυξημένες ανάγκες και να παρέχεται πρόσθετη λειτουργικότητα, τα περισσότερα δίκτυα έχουν αποκλειστικούς servers. Ένας αποκλειστικός server λειτουργεί μόνο ως server, όχι ως client. Η ρύθμιση αυτών των servers είναι βελτιστοποιημένη για την επεξεργασία αιτημάτων από clients δικτύου.

Τα δίκτυα client-server έχουν γίνει το στάνταρ μοντέλο στην δικτύωση. Καθώς τα δίκτυα αυξάνονται σε μέγεθος λόγω του αριθμού των συνδεδεμένων υπολογιστών, της φυσικής απόστασης και της κυκλοφορίας μεταξύ τους απαιτούνται συνήθως περισσότεροι του ενός server. Κατανέμοντας τα δικτυακά καθήκοντα μεταξύ αρκετών servers εξασφαλίζουμε ότι κάθε εργασία εκτελείται όσο το δυνατόν πιο αποτελεσματικά. Επίσης μειώνεται το εργασιακό φορτίο στους σε καθένα από τους server που εκτελούν δικτυακά καθήκοντα.

### Υλοποίηση της δικτύωσης στα Windows 2000

Τα Windows 2000 εξυπηρετούν τις ανάγκες ενός οργανισμού κάνοντας εύκολη την σύνδεση των ανθρώπων και των δικτύων με καινοτόμες μεθόδους μέσα από την οργάνωση σε **domain** και την υπηρεσία καταλόγου **Microsoft Active Directory** για εκτεταμένη επικοινωνία. Ένα δίκτυο Windows 2000 επιτρέπει στους οργανισμούς να βελτιώνουν την διαμοίραση των πληροφοριών και να δημιουργήσουν επαρκή υποδομή επικοινωνιών. Τα Windows 2000 περιλαμβάνουν κεντρικές υπηρεσίες διαχείρισης ασφάλειας και πληροφοριών.

### Τα στοιχεία ενός Domain



Στα Windows 2000, το domain είναι μια λογική ομαδοποίηση δικτυωμένων υπολογιστών οι οποίοι μοιράζονται μια κοινή περιοχή για την αποθήκευση πληροφοριών ασφαλείας. Ένα domain παρέχει μια προσέγγιση κεντρικής διαχείρισης πόρων δικτύου. Οι χρήστες ενός υπολογιστή μπορούν να έχουν πρόσβαση σε κοινόχρηστους πόρους σε άλλους υπολογιστές στο domain, εφόσον τους έχουν παρασχεθεί τα ανάλογα δικαιώματα. Τα domains είναι παρόμοια σε σύλληψη με τα



workgroups, αλλά παρέχουν επιπλέον χρήσιμα στοιχεία όπως περιγράφεται παρακάτω.

### Μία διαδικασία logon

Τα domains μία μόνο διαδικασία logon στους χρήστες για να έχουν πρόσβαση σε διάφορους πόρους του δικτύου, συμπεριλαμβανομένων των πόρων αρχείων, εκτυπωτών και εφαρμογών. Όλοι οι λογαριασμοί των χρηστών είναι αποθηκευμένοι σε μία κεντρική τοποθεσία.

### Ένας λογαριασμός χρήστη

Οι χρήστες σε ένα domain χρειάζονται μόνο έναν λογαριασμό για να έχουν πρόσβαση σε πόρους διάφορων υπολογιστών. (Σε αντίθεση, για τους χρήστες σε ένα workgroup απαιτείται ξεχωριστός λογαριασμός σε κάθε υπολογιστή που έχουν πρόσβαση.)

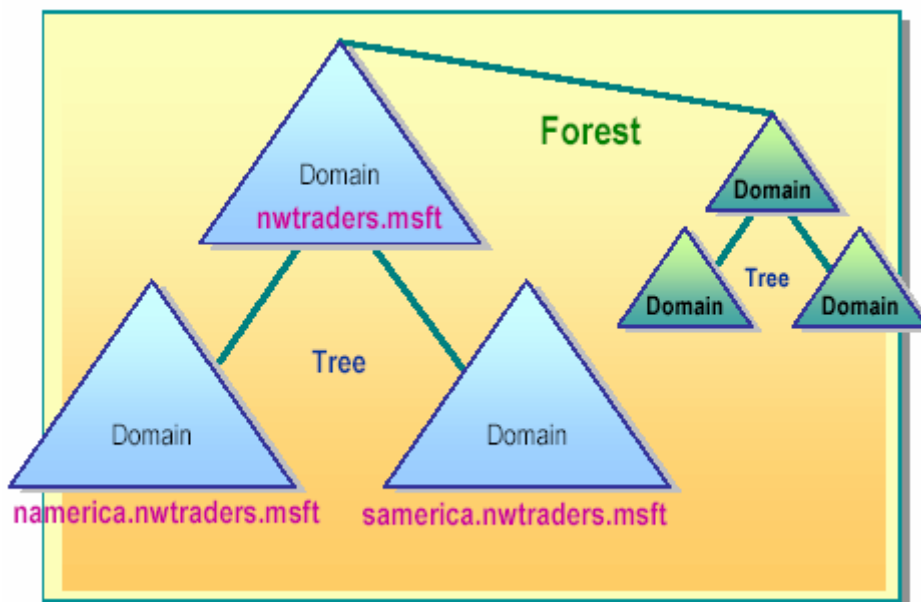
### Κεντρική διαχείριση

Τα domains παρέχουν κεντρική διαχείριση. Όλοι οι λογαριασμοί των χρηστών και οι πληροφορίες των πόρων μπορούν να διαχειρίζονται από ένα σημείο μέσα στο domain.

### Κλιμάκωση

Τα domains μπορούν να κλιμακωθούν σε πολύ μεγάλα δίκτυα. Οι τρόποι με τους οποίους οι χρήστες έχουν πρόσβαση στους πόρους και πως διαχειρίζονται οι πόροι στα πολύ μεγάλα δίκτυα είναι οι ίδιοι όπως και στα μικρά δίκτυα.

### Οργάνωση του Domain



Κάθε domain ελέγχεται από τον domain controller. Για να απλοποιηθεί ο έλεγχος πολλαπλών domains, τα domains ομαδοποιούνται σε δομές που ονομάζονται trees και forests.



## Domain Controller

Ένας υπολογιστής που τρέχει Windows 2000 Server ελέγχει καθένα domain. Αυτός ο υπολογιστής είναι γνωστός ως domain controller. Ο domain controller διαχειρίζεται όλες τις ενέργειες που έχουν σχέση με την ασφάλεια μεταξύ των χρηστών και του domain.

## Trees

Το tree είναι μια ιεραρχική διάταξη των domain των Windows 2000 τα οποία μοιράζονται ένα κοινό όνομα. Όταν προσθέτετε ένα domain σε ένα υπάρχον tree, το κάνετε sub-domain ενός domain στο tree. Αυτό το sub-domain καλείται child domain, και το domain και στο οποίο έχει προστεθεί είναι γνωστό ως το parent domain του. Αφού το child domain ενωθεί στο tree, το όνομα του προστίθεται στο όνομα του parent domain. Για παράδειγμα, όταν το domain London συμμετέχει σε ένα υπάρχον tree και γίνεται child του parent domain nwtraders.msft, το όνομα του domain του γίνεται london.nwtraders.msft.

## Forests

Το forest είναι μία ομάδα trees τα οποία δεν μοιράζονται κάποιο όνομα, αλλά μοιράζονται μια κοινή διαμόρφωση. Εξ ορισμού, το όνομα του αρχικού, ή το πρώτο tree που δημιουργείται στο forest, χρησιμοποιείται για να αναφερόμαστε στο δοσμένο forest. Για παράδειγμα, αν το nwtraders.msft είναι το πρώτο domain στο πρώτο tree και κάποιο άλλο tree συμμετέχει σ' αυτό για να φτιάξουν ένα forest, το όνομα του forest είναι nwtraders.msft.



## TROUBLESHOOTING

- Πώς μπορώ να δω την IP που έχει ένας σταθμός εργασίας αφού στην καρτέλα TCP/IP είναι ρυθμισμένος να παίρνει την διεύθυνση δυναμικά;

Ανοίγουμε ένα παράθυρο γραμμής εντολών και γράφουμε την εντολή ipconfig, (σε windows 9x η αντίστοιχη εντολή είναι η winipcfg).

- Πώς μπορώ να ελέγξω αν ένας σταθμός εργασίας μπορεί να επικοινωνήσει με τον DHCP server και να ανανεώσει την IP του;

Στην γραμμή εντολών πληκτρολογούμε ipconfig /release και μετά ipconfig /renew. Αν αποδοθεί διεύθυνση IP τότε δεν υπάρχει πρόβλημα επικοινωνίας ή λειτουργίας του DHCP server. Σε win 9x γράφουμε winipcfg και πατάμε τα κουμπιά «απελευθέρωση» και «ανανέωση».

- Η τηλεφωνική γραμμή ανοίγει αλλά ο browser δεν ανοίγει δικτυακές τοποθεσίες.

1) Δοκιμάζουμε να ανοίξουμε έναν δικτυακό τόπο με την ip διεύθυνσή του. Το www.sch.gr π.χ. έχει ip την 194.63.238.73. Αν ανοίξει τότε υπάρχει πρόβλημα με DNS server.

2) Ελέγχουμε αν υπάρχουν ρυθμίσεις για proxy server και αν είναι έγκυρες.

- Πώς μπορώ να δω αν ένας σταθμός εργασίας είναι συνδεδεμένος με διάφορες τοποθεσίες στο internet ενώ είναι κλειστός ο browser ή το πρόγραμμα αλληλογραφίας;

Στην γραμμή εντολών πληκτρολογούμε netstat. Η έξοδος αυτής της εντολής θα μας δείξει ποιες συνδέσεις υπάρχουν και σε ποιες θύρες. Αυτή η εντολή είναι χρήσιμη για τον εντοπισμό κακόβουλων προγραμμάτων / ιών που τρέχουν στο παρασκήνιο και επικοινωνούν με διάφορες τοποθεσίες στο Internet.



## DNS

η συντομογραφία των λέξεων **Domain Name System**.

### **Ο ρόλος του DNS Server**

Λίγα λόγια πριν. Όλοι οι υπολογιστές που δεν είναι αυτόνομοι, για να συνδεθούν μεταξύ τους και να «καλεί» ο ένας τον άλλον, χρησιμοποιούν πρωτόκολλα επικοινωνίας. Το πιο διαδεδομένο μέχρι σήμερα και αυτό στο οποίο βασίζεται και το internet, ονομάζεται TCP/IP. Με αυτό το πρωτόκολλο κάθε Η/Υ αποκτά ένα μοναδικό, πολυσύνθετο αριθμό. Για την ακρίβεια αποκτά τέσσερις τριψήφιους αριθμούς που θεωρητικά μπορούν να πάρουν τιμές από το 1 έως και το 255. Σύμφωνα με τα παραπάνω, αν θέλουμε να καλέσουμε ένα τυχαίο υπολογιστή π.χ. τον server του πανεπιστημίου Μακεδονίας και που η ονομασία του είναι <http://www.uom.gr> μπορούμε κάλλιστα να τον καλέσουμε και σαν <http://195.251.213.107/>, αν το θυμόμαστε βέβαια. Το ορθόν είναι βέβαια να καλέσουμε το δεύτερο, αφού το πρώτο είναι μία «επιγραφή» Επειδή όπως καταλαβαίνετε κάτι τέτοιο είναι αδύνατο για ένα υπολογιστή φανταστείτε για περισσότερους. Γι' αυτό τον λόγο επινοήθηκαν οι DNS servers ή τα DNS Services, δηλαδή υπολογιστές ή διαδικασίες που επεμβαίνουν αυτόματα κάθε φορά που εμείς καλούμε έναν υπολογιστή και μεταφράζουν τις επιγραφές στις κανονικές τους διευθύνσεις. Οι υπολογιστές που αναλαμβάνουν αυτή την δουλειά είναι και αυτοί συνδεδεμένοι μεταξύ τους σε ένα δικό τους δίκτυο. Έτσι όταν κάποιος DNS server δεν μπορεί να μεταφράσει την επιγραφή σε διεύθυνση προωθεί το αίτημα της κλίσης μας σε άλλον, διαδικασία γνωστή αλλιώς και σαν «forward». Η διαδικασία «forward» μπορεί να επαναληφθεί, αν χρειαστεί, τόσες φορές όσες θα χρειάζεται για να μεταφραστεί το αίτημά μας και να επιστρέψει σε εμάς.

***Ρυθμίζοντας – Παραμετροποιώντας τον server.***



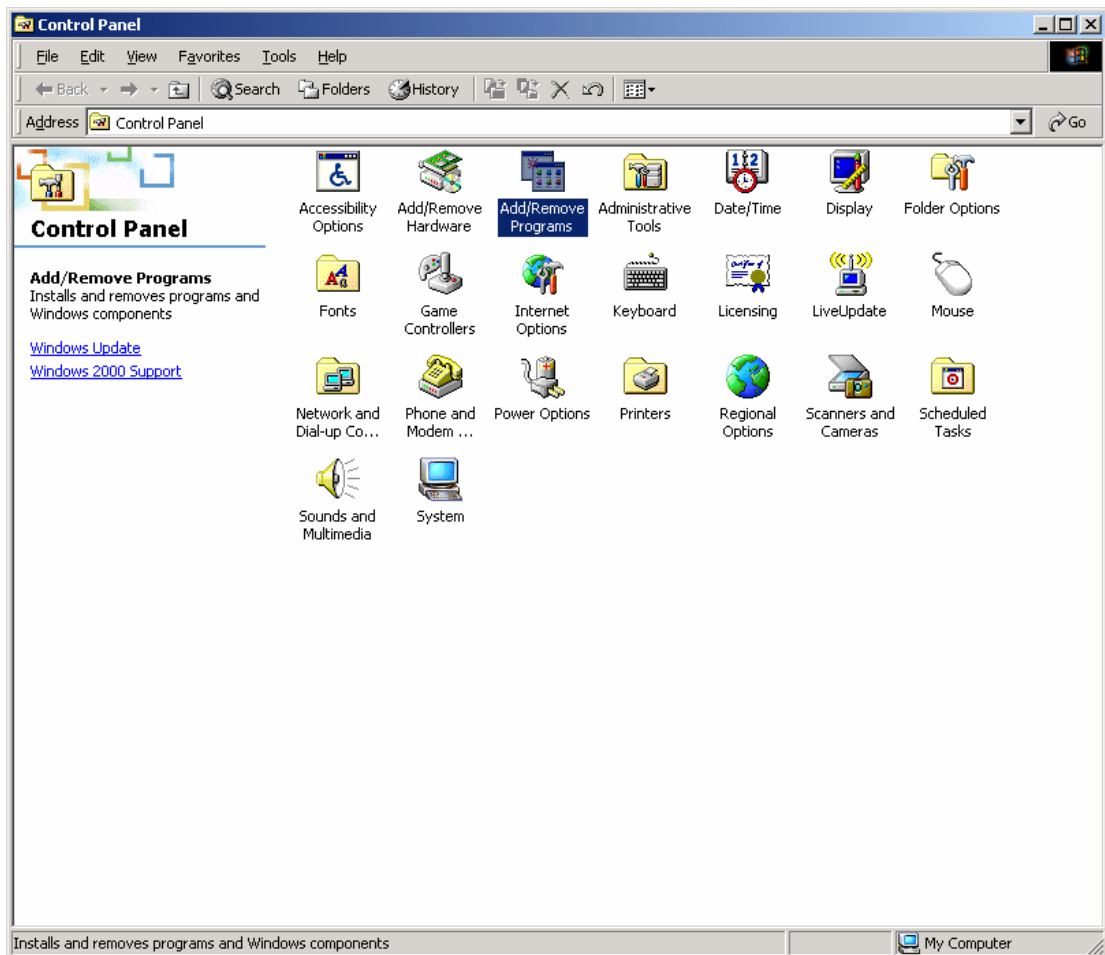


## Windows2000 Server - Εγκατάσταση και ρυθμίσεις υπηρεσίας DNS- Αναλυτικές οδηγίες

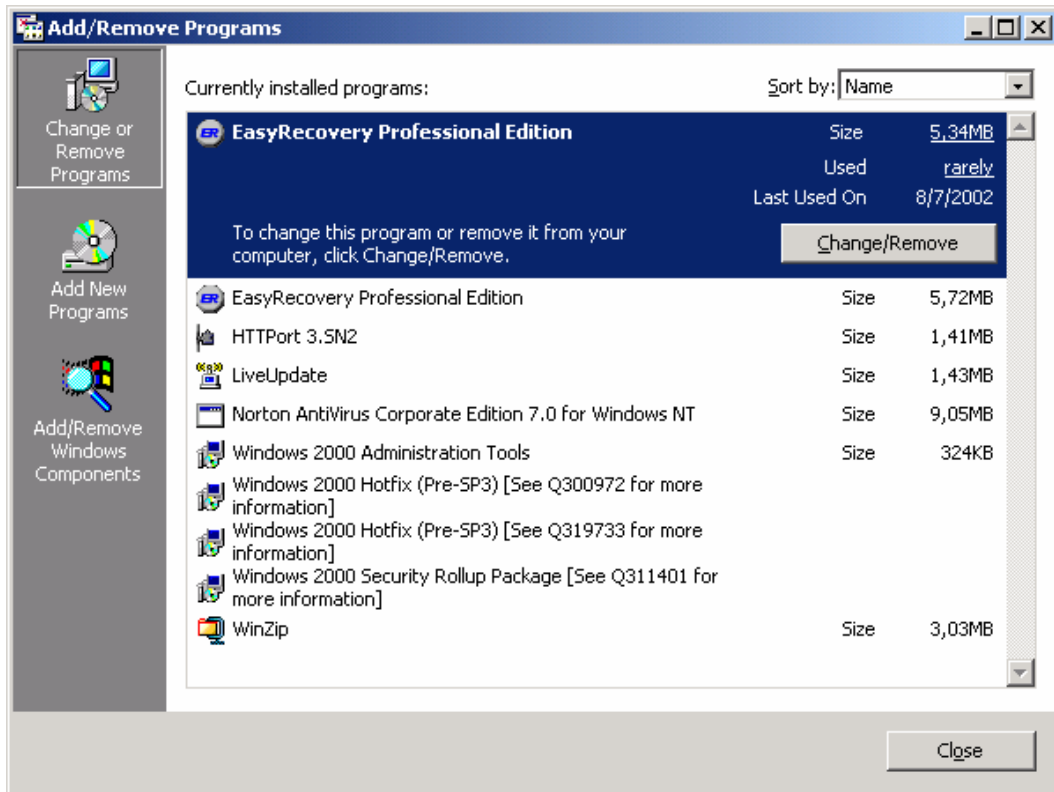
### *Εγκατάσταση της υπηρεσίας DNS*

Αν δεν είναι εγκατεστημένη η υπηρεσία DNS προχωράμε στην εγκατάσταση της. Για την εγκατάσταση θα πρέπει να υπάρχει διαθέσιμο το CD των Windows 2000 Server.

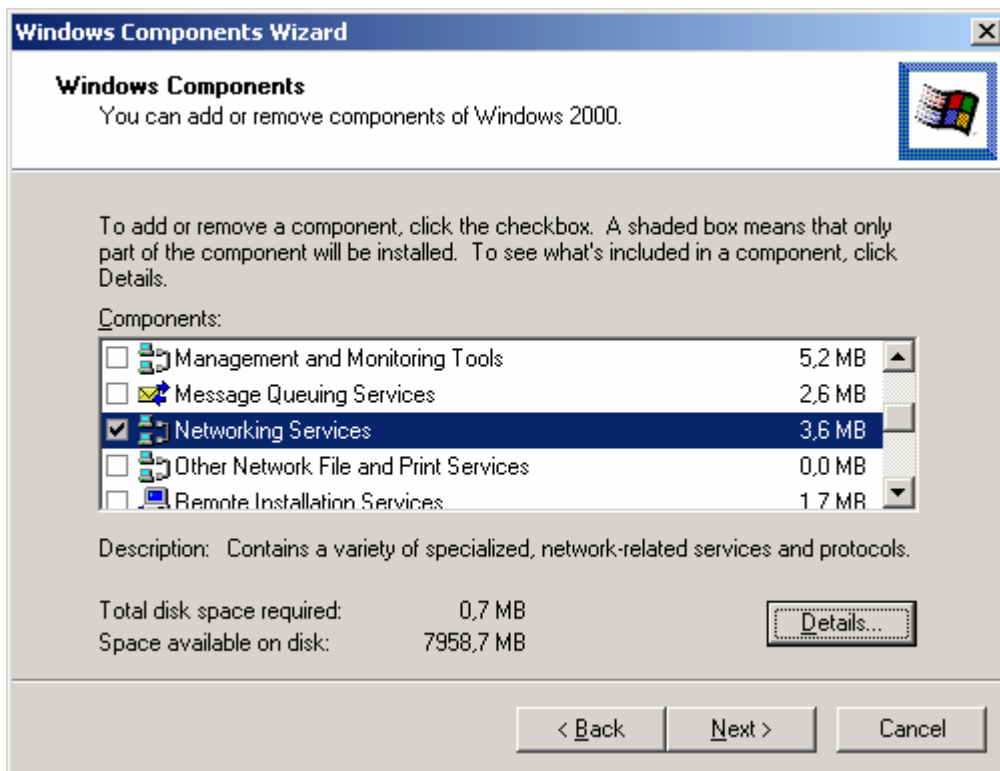
Από το πλήκτρο Start των Windows επιλέγουμε Settings/Control Panel



Διπλοπατάμε στο Add/Remove Programs, οπότε εμφανίζεται η ακόλουθη οθόνη.

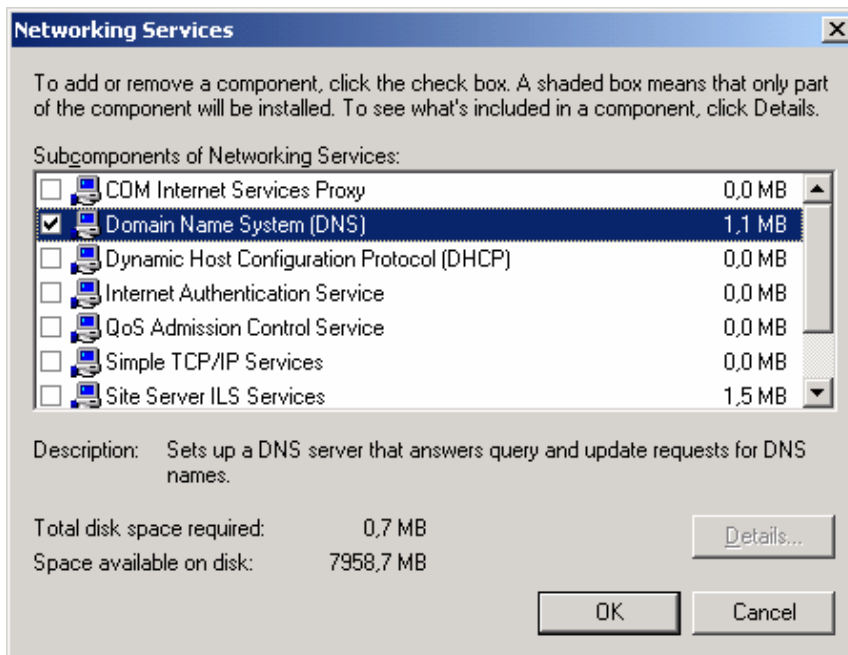


Πατάμε Add/Remove Windows Components οπότε εμφανίζεται το πλαίσιο διαλόγου της επόμενης εικόνας





Πατάμε Details, οπότε εμφανίζεται το πλαίσιο της επόμενης εικόνας.



#### Σημείωση

Αν είναι ήδη check box Domain Name System (DNS) επιλεγμένο σημαίνει ότι η υπηρεσία DNS είναι εγκατεστημένη οπότε εγκαταλείπουμε την διαδικασία με **Cancel**.

Επιλέγουμε το check box Domain Name System (DNS).

Και πατάμε το πλήκτρο **OK** οπότε επιστρέφουμε στην προηγούμενη εικόνα, στην οποία συνεχίζουμε την εγκατάσταση με το πλήκτρο **Next**.

Θα ζητηθεί το CD των Windows

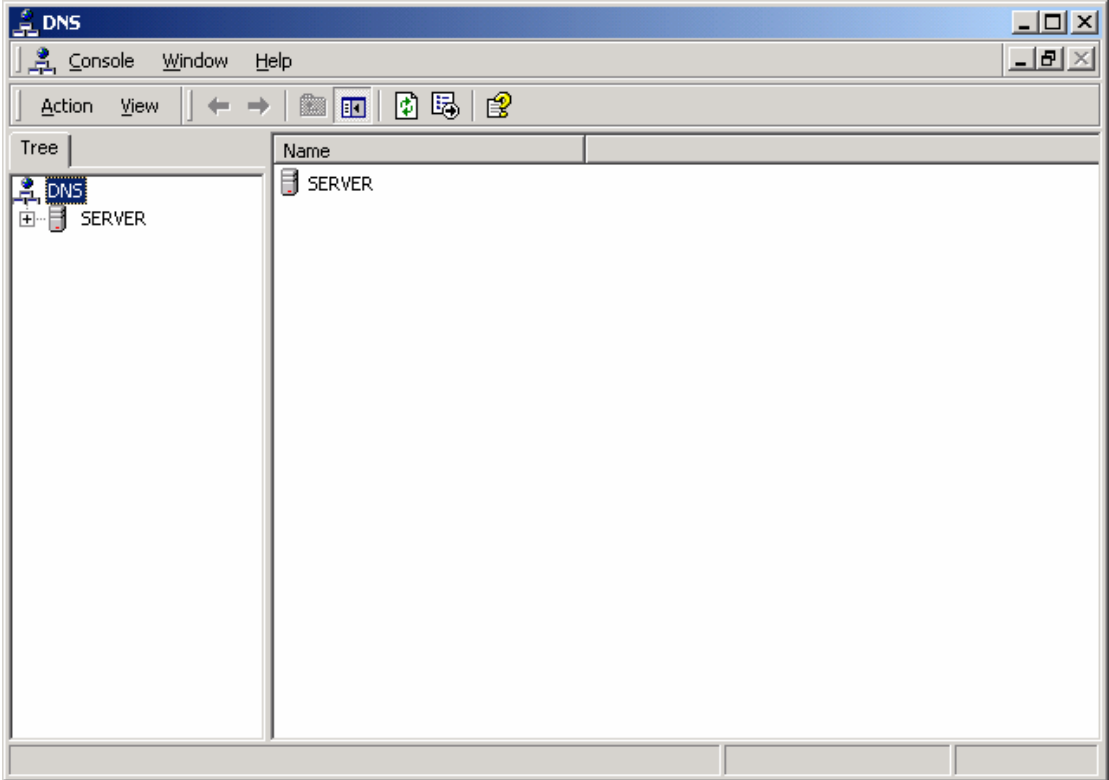
Βάζουμε το CD και ολοκληρώνεται η διαδικασία εγκατάστασης της υπηρεσίας DNS με το μήνυμα .



Πατάμε **Finish**

### *Ρυθμίσεις της υπηρεσίας DNS.*

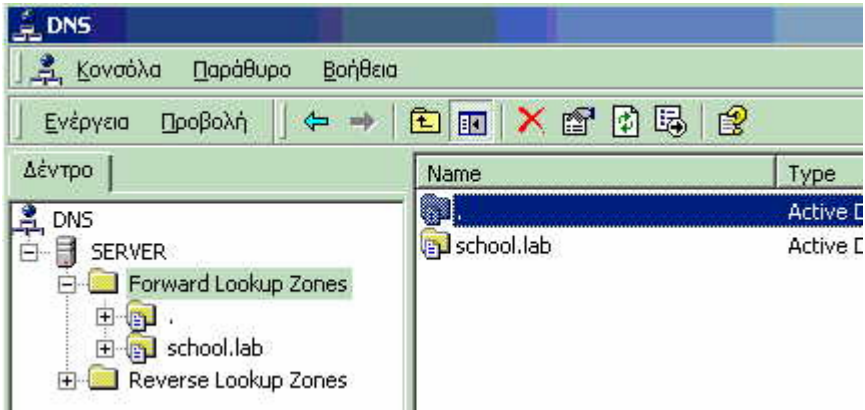
Οι ρυθμίσεις γίνονται από την DNS console η οποία ενεργοποιείται από το Menu Start με την ακολουθία **Start/Programs/ Administrative Tools/DNS**.  
Εμφανίζεται η ακόλουθη console.



**Ορισμός Forwarders**

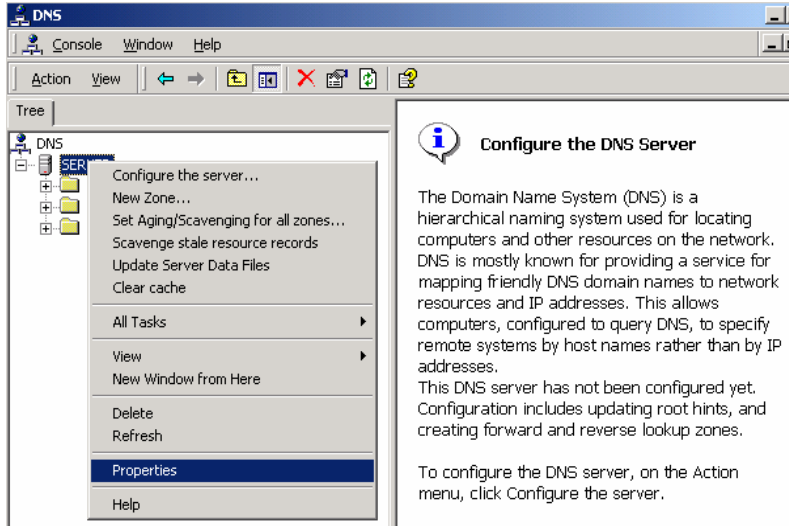
Στα Services του εξυπηρετητή, εάν το DNS service δεν λειτουργεί, εκκίνηση του Microsoft DNS Service

Στην διαχείριση του DNS Service[Administrative Tools ->DNS], αν υπάρχει η ζώνη «.» στις Forward Lookup Zones την διαγράφουμε



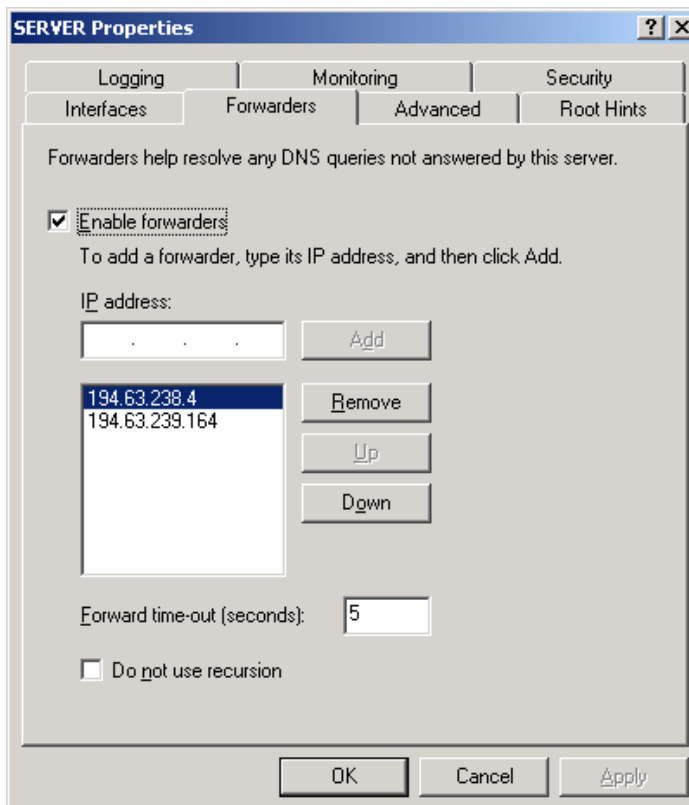
και σταματάμε (STOP) και επανεκκινούμε (START) το Microsoft DNS Service

Στην console πατάμε δεξί πλήκτρο και επιλέγουμε properties.



Στο εμφανιζόμενο πλαίσιο και στην καρτέλα forwarders ορίζουμε ως forwarders Forwarders ιεραρχικά τους πλησιέστερους DNS servers με την μονάδα. (Νομαρχιακός Κόμβος αν υπάρχει -1<sup>ος</sup> πλησιέστερος δικτυακά Περιφερειακός κόμβος ή 1<sup>ος</sup> πλησιέστερος δικτυακά Περιφερειακός κόμβος - 2<sup>ος</sup> Περιφερειακός κόμβος) σύμφωνα με την πιο κάτω εικόνα

**Όλα τα άλλα πεδία μένουν στις Default ρυθμίσεις .**





## Ορισμός Forward Lookup Zone

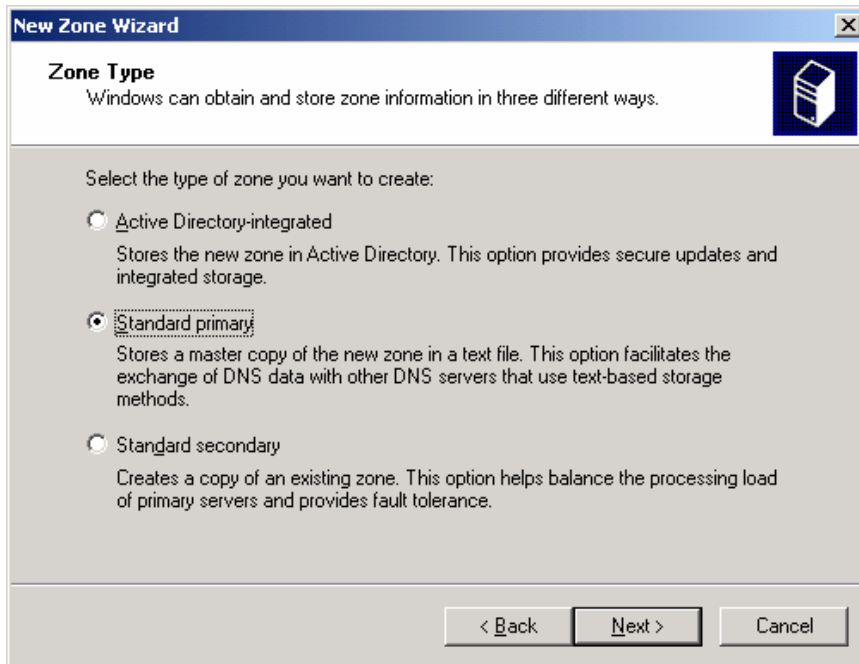
### Ορισμός ζώνης

1. Αναπτύσσουμε τον κλάδο SEVER ώστε να είναι ορατοί ο κλάδος Forward Lookup zones πατώντας στο σύμβολο [+] που υπάρχει μπροστά από το όνομα του DNS SERVER.
2. Πατάμε με το δεξί πλήκτρο πάνω στο **Forward Lookup Zones** και επιλέγουμε new Zone. Ακολουθούμε τα βήματα του Wizard για την δημιουργία της ζώνης.

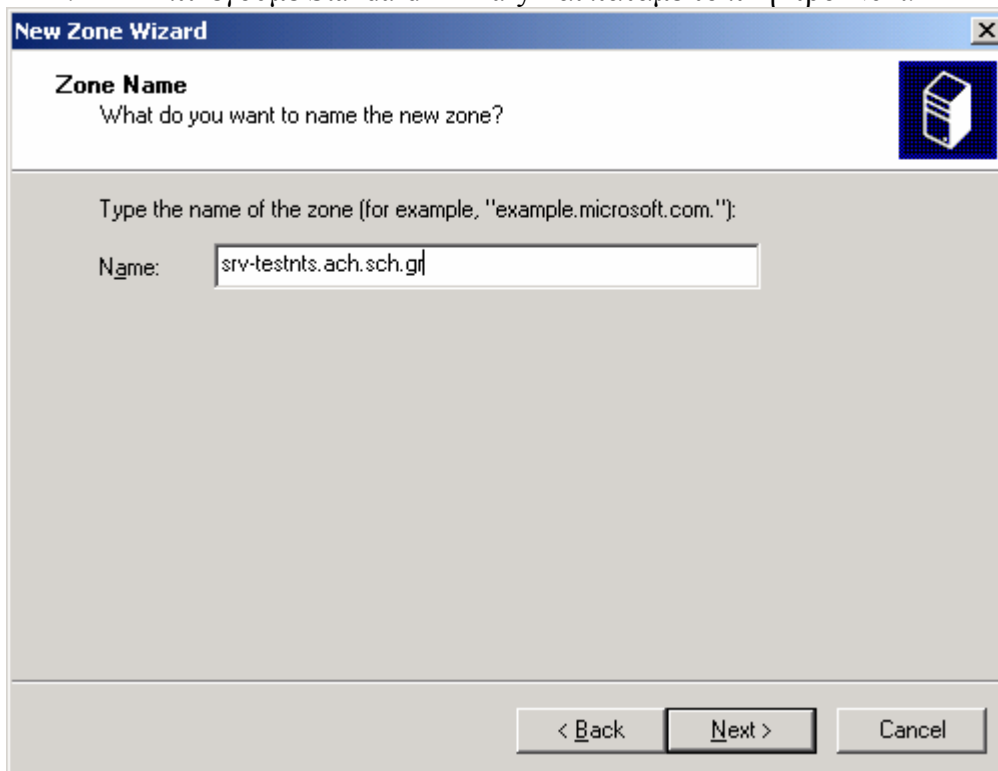


3. Πατάμε το πλήκτρο επόμενο



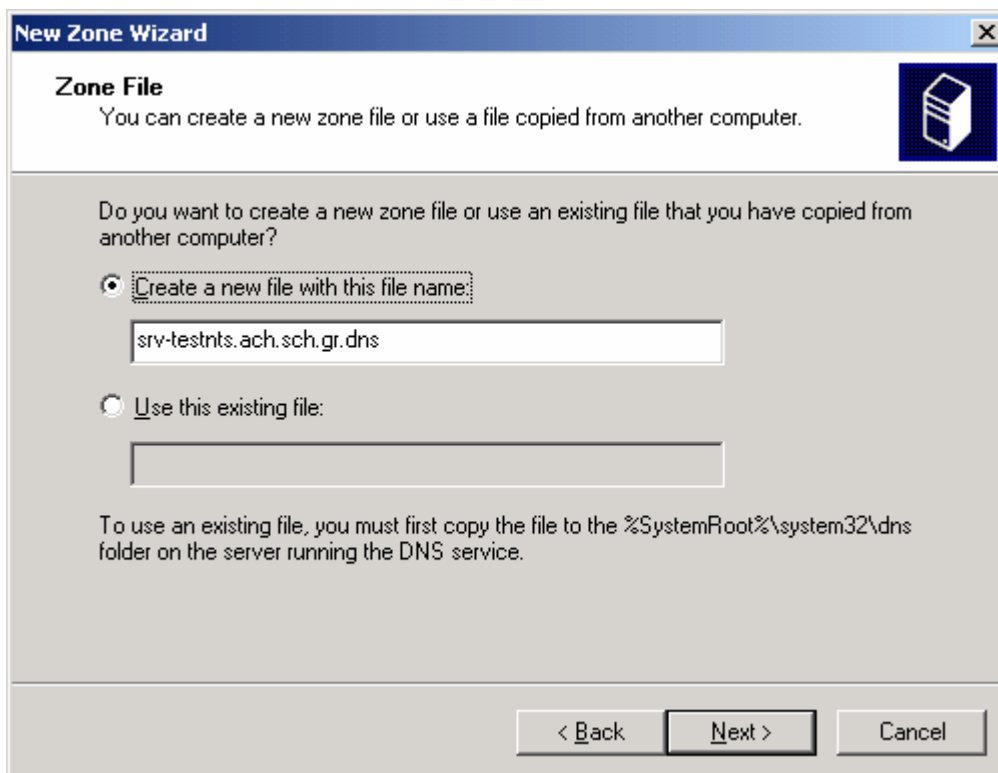


4. Επιλέγουμε Standard Primary και πατάμε το πλήκτρο Next.



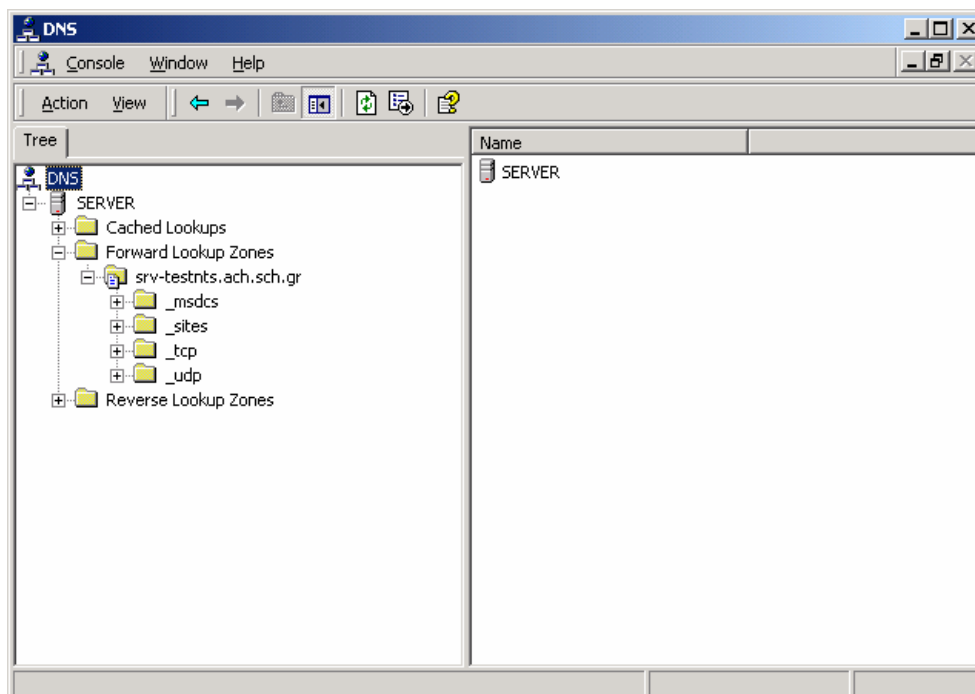
5. Συμπληρώνουμε το όνομα της ζώνης. Ως όνομα ζώνης δίνουμε το srv-  
<FQDN σχολείου> . Πατάμε το πλήκτρο Next.

6. Next στο επόμενο μήνυμα Και τέλος Finish

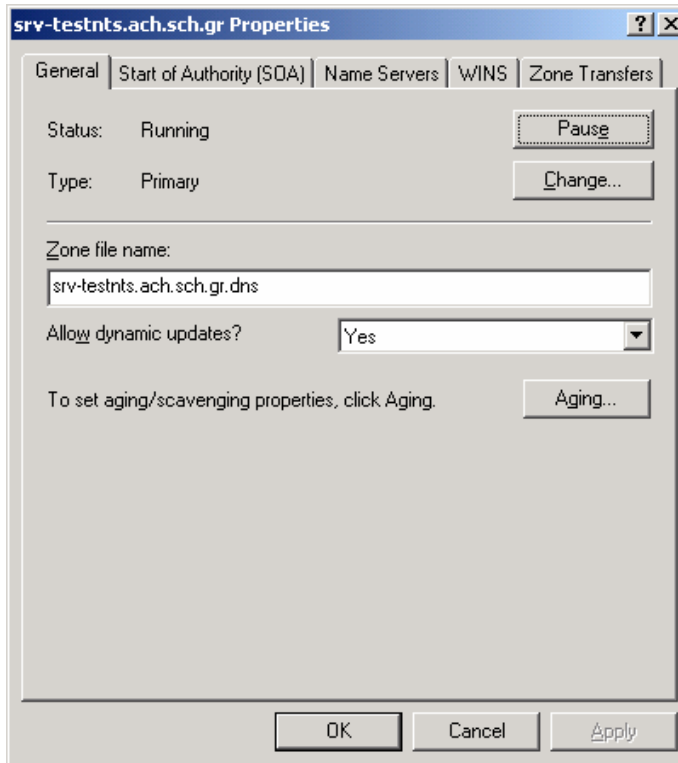


### Ρύθμιση ιδιοτήτων ζώνης

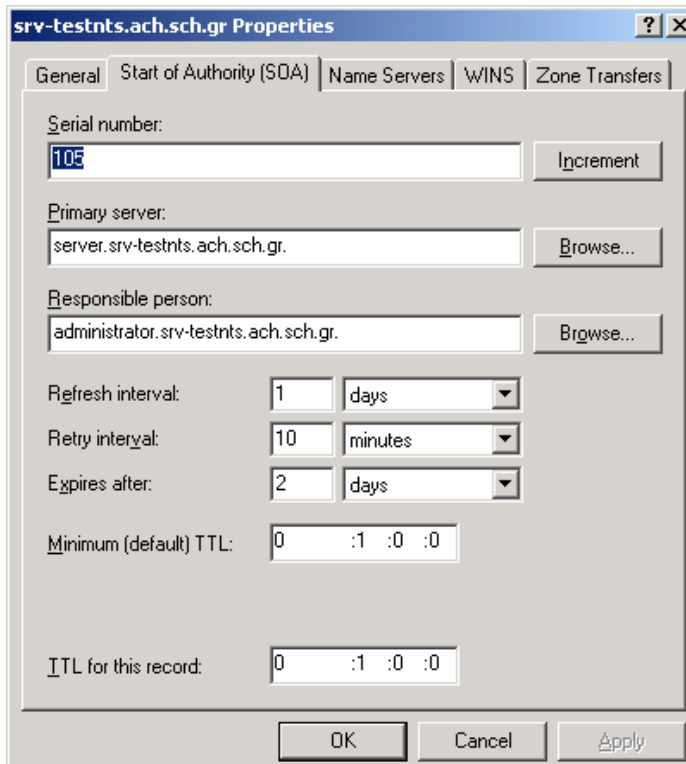
Στην ζώνη που δημιουργήσαμε πατάμε δεξί πλήκτρο και επιλέγουμε **properties**.



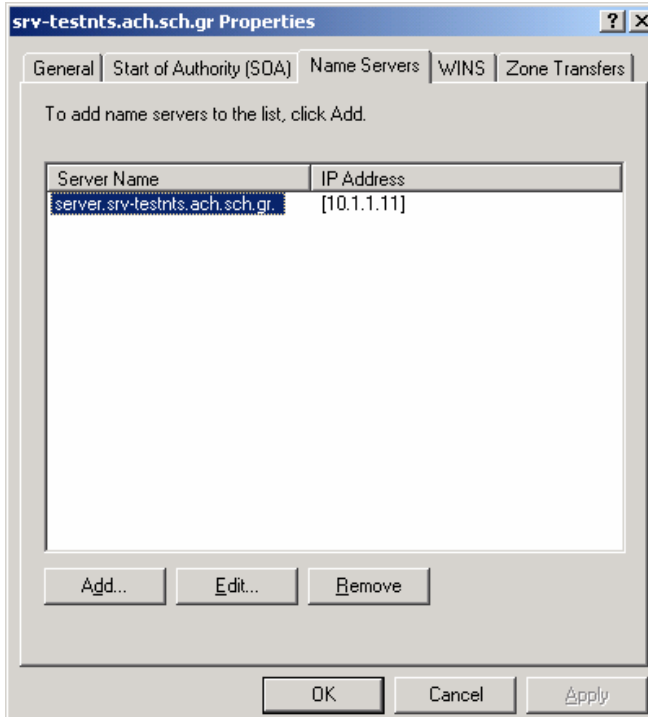
Μεγάλη προσοχή στην επιλογή “Allow dynamic updates” την οποία κάνουμε “yes”



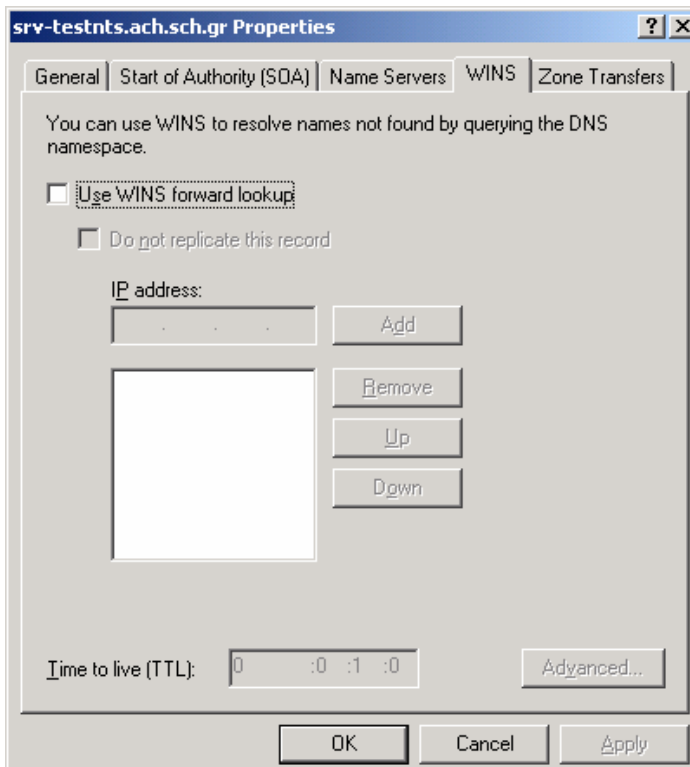
Στην καρτέλα SOA αφήνουμε τις τυπικές τιμές



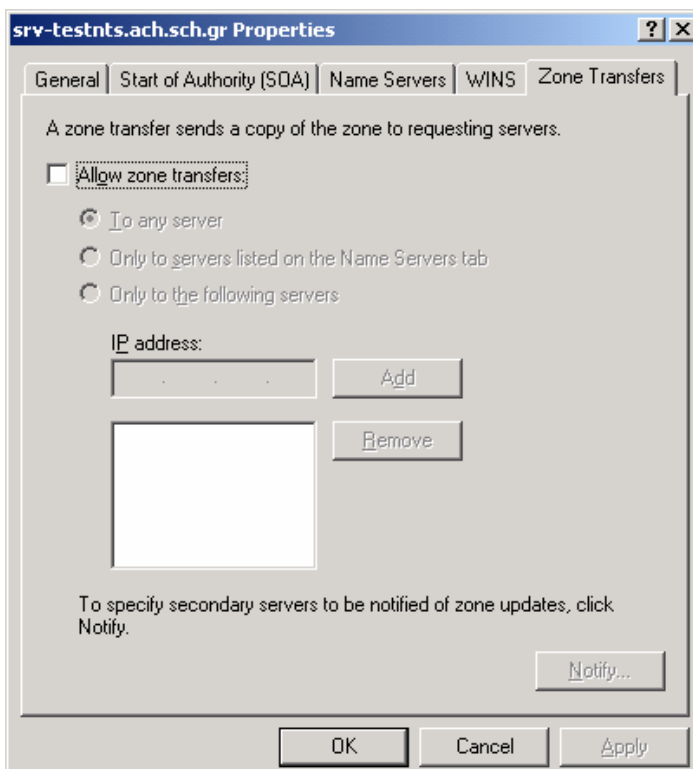
Name server για την ζώνη είναι ο server του σχολικού εργαστηρίου μόνο.



Αποεπιλέγουμε το Use WINS forward lookup



Αποεπιλέγουμε το Allow zone transfer



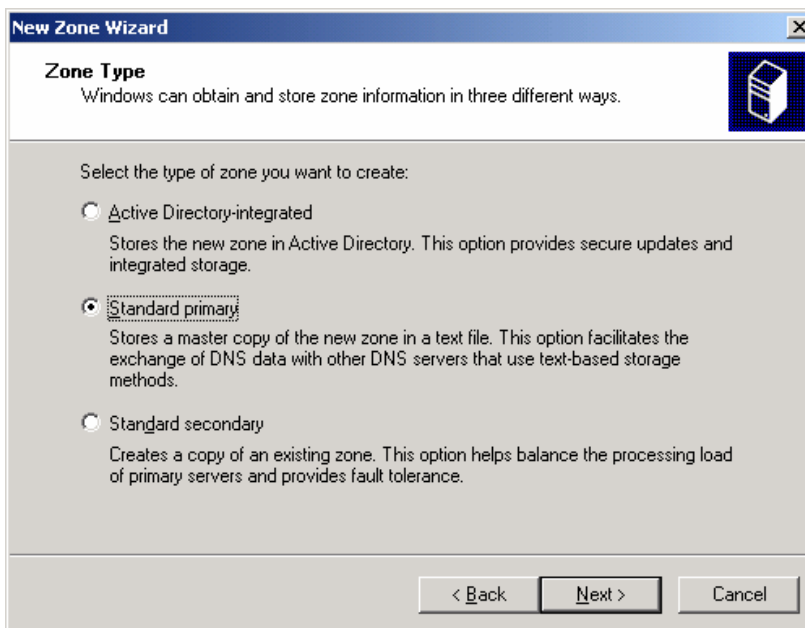
## Reverse Lookup Zones

### Ορισμός ζώνης

1. Αναπτύσσουμε τον κλάδο SEVER ώστε να είναι ορατοί ο κλάδος Forward Lookup zones πατώντας στο σύμβολο [+] που υπάρχει μπροστά από το όνομα του DNS SERVER.
2. Πατάμε με το δεξί πλήκτρο πάνω στο **Reverse Lookup Zones** και επιλέγουμε new Zone. Ακολουθούμε τα βήματα του Wizard για την δημιουργία της ζώνης.



3. Πατάμε το πλήκτρο επόμενο



4. Επιλέγουμε Standard Primary και πατάμε το πλήκτρο Next.

5. Συμπληρώνουμε το δίκτυο . Ως Network Id συμπληρώνουμε το Network number του private δίκτυου που έχει αποδοθεί στην μονάδα. **10.x.y**



**New Zone Wizard**

**Reverse Lookup Zone**  
A reverse lookup zone is an address-to-name database that helps computers translate IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

Network ID:  
10 .1 .1| .

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 169 would create zone 169.in-addr.arpa, and network ID 169.0 would create zone 0.169.in-addr.arpa.

Reverse lookup zone name:  
1.1.10.in-addr.arpa

< Back   Next >   Cancel

6. Next στην επόμενη οθόνη μήνυμα και τέλος Finish

**New Zone Wizard**

**Zone File**  
You can create a new zone file or use a file copied from another computer.

Do you want to create a new zone file or use an existing file that you have copied from another computer?

Create a new file with this file name:  
1.1.10.in-addr.arpa.dns

Use this existing file:  
\_\_\_\_\_

To use an existing file, you must first copy the file to the %SystemRoot%\system32\dns folder on the server running the DNS service.

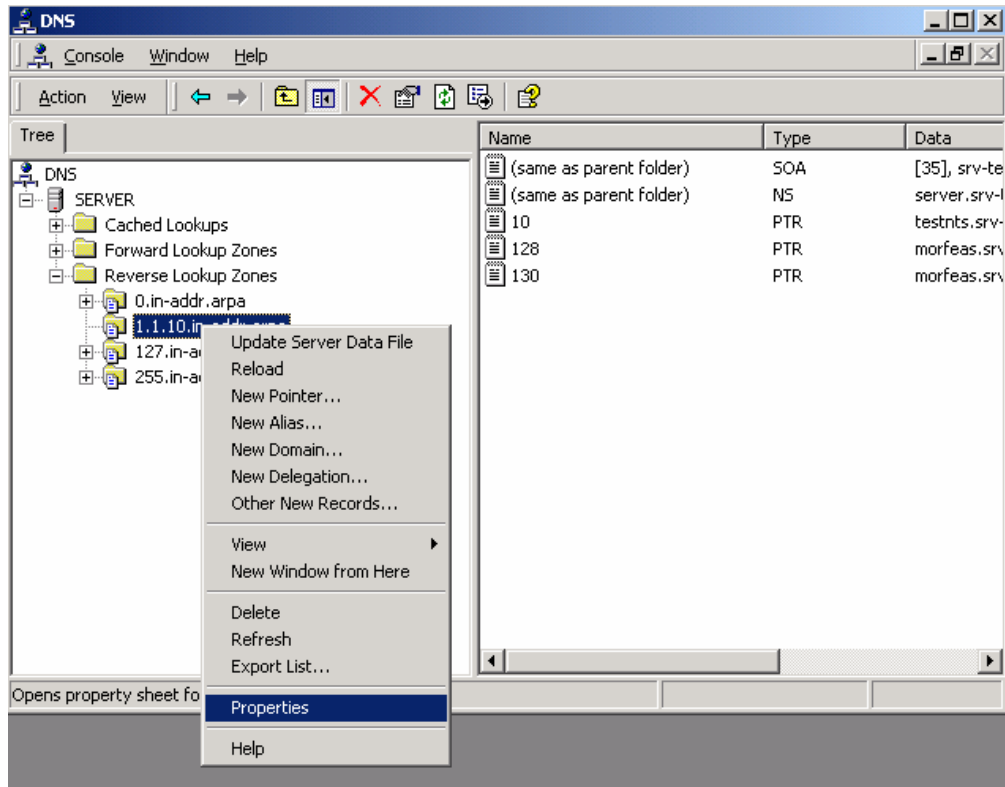
< Back   Next >   Cancel



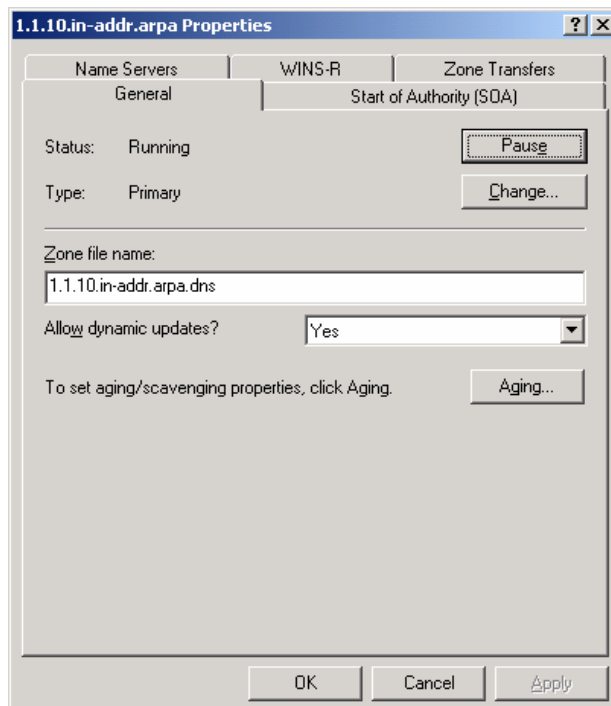


### Ρύθμιση ιδιοτήτων ζώνης

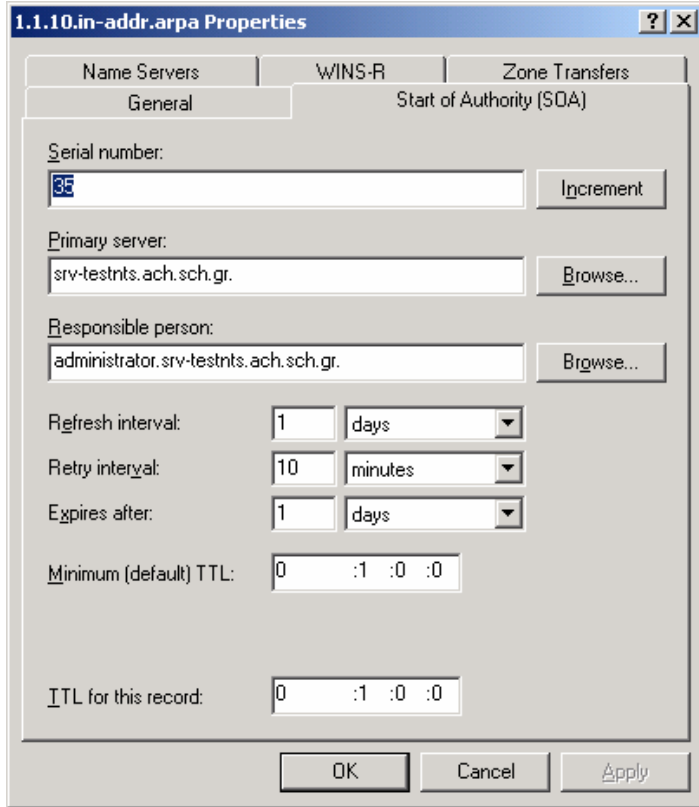
Απαιτείται η ρύθμιση των ιδιοτήτων στη reverse ζώνη με ανάλογο τρόπο όπως και στην forward.



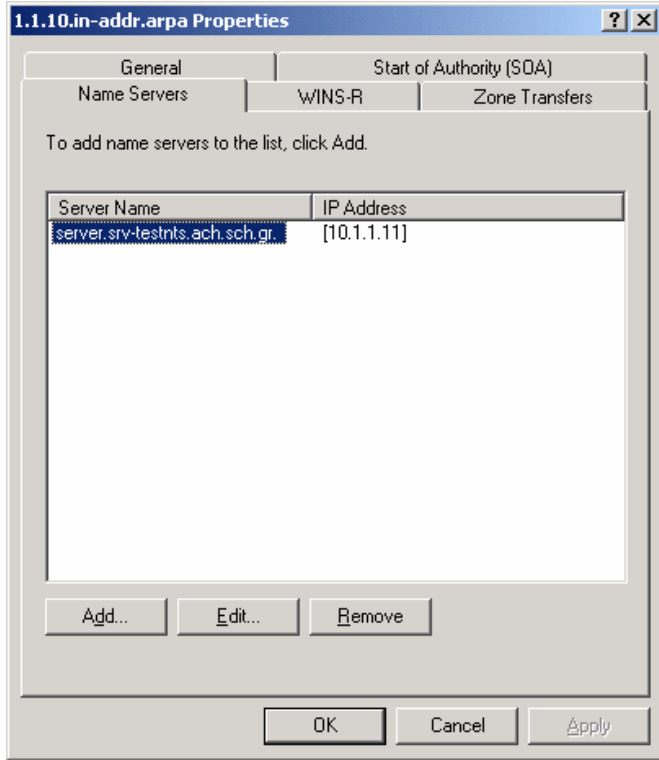
Μεγάλη προσοχή στην επιλογή “Allow dynamic updates” την οποία κάνουμε “yes”



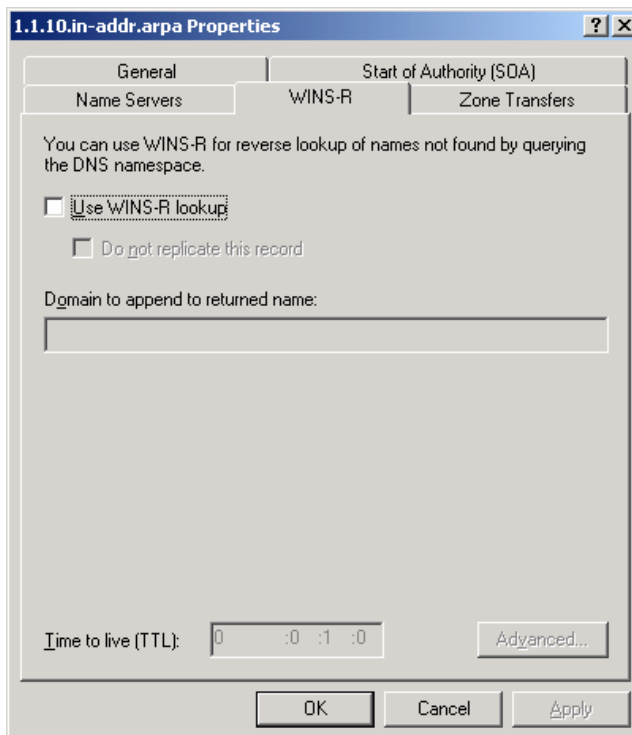
Στην καρτέλα SOA αφήνουμε τις τοπικές τιμές



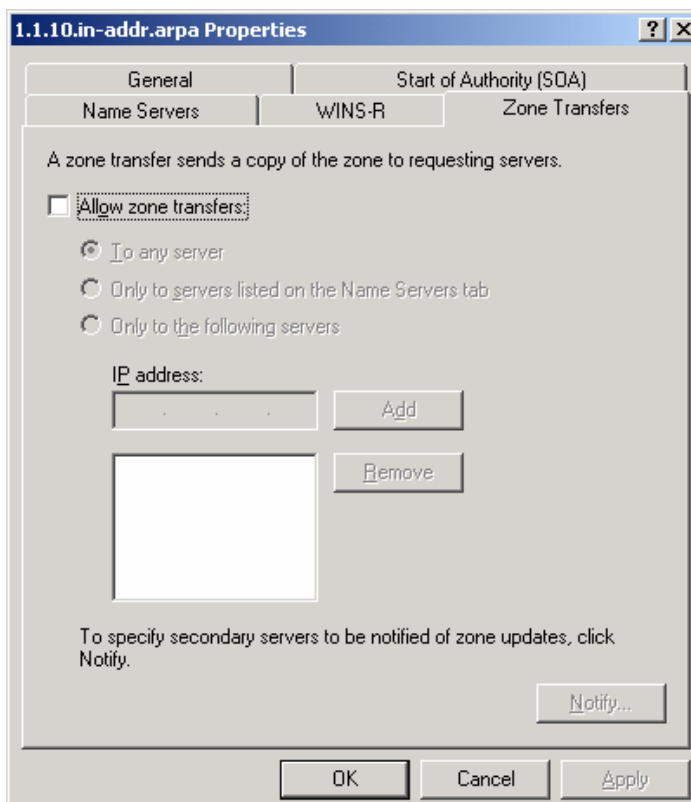
Name server για την ζώνη είναι ο server του σχολικού εργαστηρίου μόνο.



Αποεπιλέγουμε το Use WINS forward lookup



Αποεπιλέγουμε το Allow zone transfer





## Troubleshooting

➤ **Έχω τον Server ανοικτό και παρόλα αυτά ενώ ξέρω ότι το γενικότερο δίκτυο (Edunet) δεν έχει πρόβλημα δεν βλέπω Ιντερνετ**

- Ελέγχω αν ζητάω σελίδες μέσω proxy server(internet explorer – tools – internet options-connections-lan settings), και αν ναι βλέπω αν είναι εγκατεστημένος κάποιος proxy στον Server (πχ ISA SERVER). Αν δεν είναι απενεργοποιώ την σύνδεση μέσω proxy server στον Internet explorer
- Βλέπουμε μέσα στην υπηρεσία DNS του SERVER αν οι ρυθμίσεις στην καρτέλα Forwarders είναι σωστές.(προσοχή αν οι διευθύνσεις που βάζουμε εκεί είναι σωστές)

➤ **Όταν κλείνω τον Server δεν έχουν πρόσβαση στο Ιντερνετ οι Clients**

- σε παράθυρο command prompt γράφω την εντολή ipconfig/all . Παρατηρώ το πεδίο που αναφέρεται στο DNS και βλέπω αν υπάρχουν και άλλοι DNS servers εκτός του σχολικού μας Server. Αν δεν υπάρχει κάποιος εναλλακτικός DNS Server ειδοποιώ το Edunet .



## DHCP

συντομογραφία των λέξεων Dynamic Host Configuration Protocol.

### ***ρόλος του DHCP Server***

DHCP server ή service είναι ένας υπολογιστής, ένας router ή μία διεργασία η οποία αναλαμβάνει όταν της ζητηθεί να αποδώσει διεύθυνση IP στον αιτούντα. Στα υπάρχοντα σχολεία και όπου υπάρχει δίκτυο αυτήν την διεργασία την έχει επιφορτιστεί ο δρομολογητής ή αλλιώς router. Έτσι κάθε φορά που ξεκινάει οποιοσδήποτε υπολογιστής κάνει αίτηση σε όλο το τοπικό δίκτυο για να του αποδοθεί διεύθυνση IP. Ο server ή ο router που αναλαμβάνει μια τέτοια υπηρεσία συνήθως μοιράζει και άλλες πληροφορίες όπως για παράδειγμα την διεύθυνση δικτυακού εκτυπωτή κ.α.

### ***Troubleshooting***

- **Στον router για κάποιο λόγο δεν ανταποκρίνεται η υπηρεσία dhcp. Αποτέλεσμα αυτού είναι οι υπολογιστές να παίρνουν τυχαίες διευθύνσεις και να μην λειτουργεί το εσωτερικό δίκτυο. Υπάρχει τρόπος να δοθούν σωστές διευθύνσεις μέχρι να αποκατασταθεί ο router?**
- Μπορούν να δοθούν στατικές διευθύνσεις στους υπολογιστές ίδιας κλάσης με του Server που έχει στατική διεύθυνση
- Μπορεί να σηκωθεί υπηρεσία DHCP από τον Server

**ΠΡΟΣΟΧΗ!!!** Και οι δύο παραπάνω ενέργειες πρέπει να γίνουν εν γνώσει του φορέα υλοποίησης



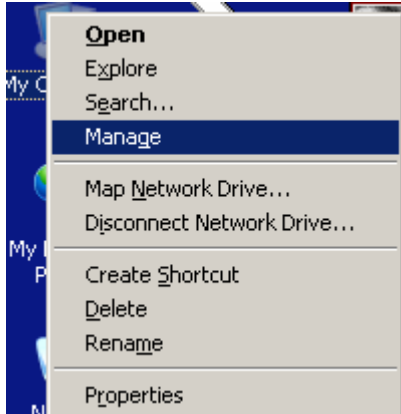
## Τοπικοί χρήστες - ομάδες

### **Local – Domain user (τοπικός χρήστης- χρήστης τομέα)**

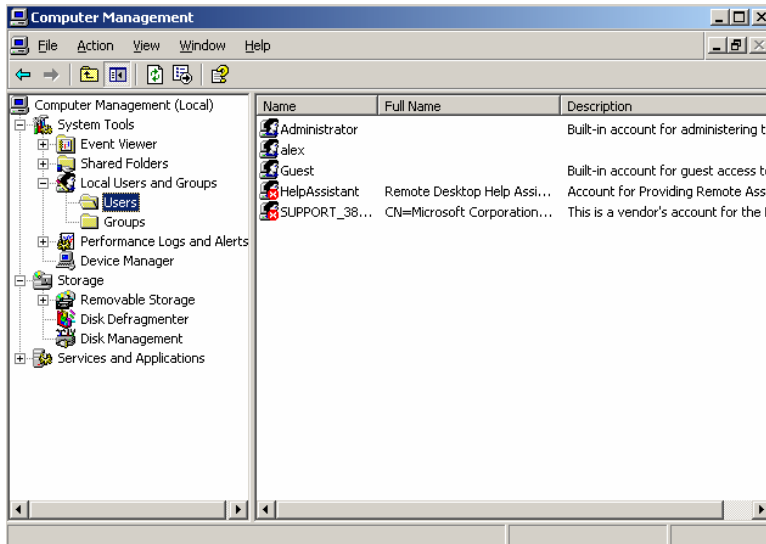
Υπάρχει μεγάλη διαφορά στην έννοια του τοπικού χρήστη και του χρήστη τομέα. Ο τοπικός χρήστης είναι ένας χρήστης του οποίου τα χαρακτηριστικά φυλάσσονται σε συγκεκριμένο υπολογιστή, διαχειρίζονται από εκεί και προφανώς ο χρήστης αυτός έχει πρόσβαση μόνο στον συγκεκριμένο υπολογιστή ο οποίος ουσιαστικά δεν κάνει logon στο domain που υπάρχει, αλλά κάνει τοπικά στον υπολογιστή χάνοντας έτσι τα προνόμια που έχει ένα δίκτυο με server. (επιλογή από το μενού log on to το όνομα του υπολογιστή και όχι του domain). Ένας χρήστης του τομέα είναι ένας χρήστης που τα χαρακτηριστικά του φυλάσσονται στον domain controller, μέσα στο active directory, από εκεί διαχειρίζονται τα χαρακτηριστικά του και ο χρήστης μπορεί να έχει πρόσβαση σε όλους τους υπολογιστές του τομέα, εκτός και αν ο διαχειριστής αποφασίσει αλλιώς. Έχει όλα τα προνόμια ενός δικτύου με server όπως πχ τα έγγραφα του να σώζονται στον server και σε οποιοδήποτε υπολογιστή και αν κάνει log on θα βλέπει τα ίδια έγγραφα. Κατά την διαδικασία log on στο μενού log on to επιλέγεται το όνομα του τομέα.

### **Δημιουργία – διαχείριση τοπικών χρηστών και ομάδων**

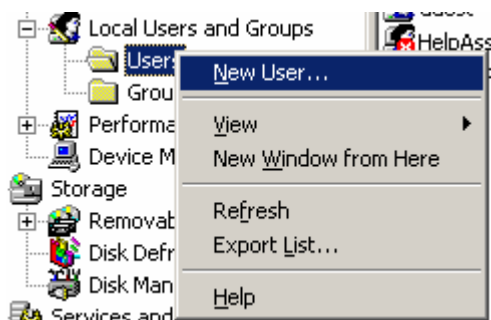
Καταρχήν θα πρέπει να γίνει μία επεξήγηση της έννοιας **ομάδα (group)**. Group ονομάζουμε μία ομάδα που μπορεί να περιέχει πολλούς χρήστες, υπολογιστές και γενικά αντικείμενα του τομέα μας. Δεν έχει δικά του χαρακτηριστικά. Για παράδειγμα μπορούμε να βάλουμε όλους τους μαθητές της πρώτης τάξης σε ένα group με όνομα class A, χωρίς αυτό να επηρεάσει τα χαρακτηριστικά του κάθε χρήστη της πρώτης τάξης. Ο λόγος που γίνεται αυτό είναι καθαρά για λόγους διαχειριστικούς. Για παράδειγμα θέλω όλοι οι μαθητές του 1 λυκείου να μπορούν να εκτυπώνουν έγγραφα. Αντί να δώσω αυτό το δικαίωμα σε καθένα από τους μαθητές δίνω το δικαίωμα στο group τους. Σε αυτή την παράγραφο θα ασχοληθούμε με την δημιουργία τοπικών χρηστών και ομάδων. Για την δημιουργία νέου χρήστη σε windows2000 – windowsXp κάνουμε δεξί κλικ πάνω στο εικονίδιο «ο υπολογιστής μου (my computer)» και επιλέγουμε διαχείριση (manage)



στην συνέχεια επιλέγουμε το μενού Local users and groups και την υποκατηγορία users

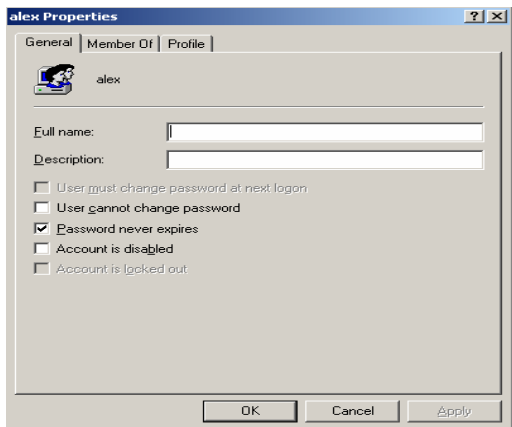
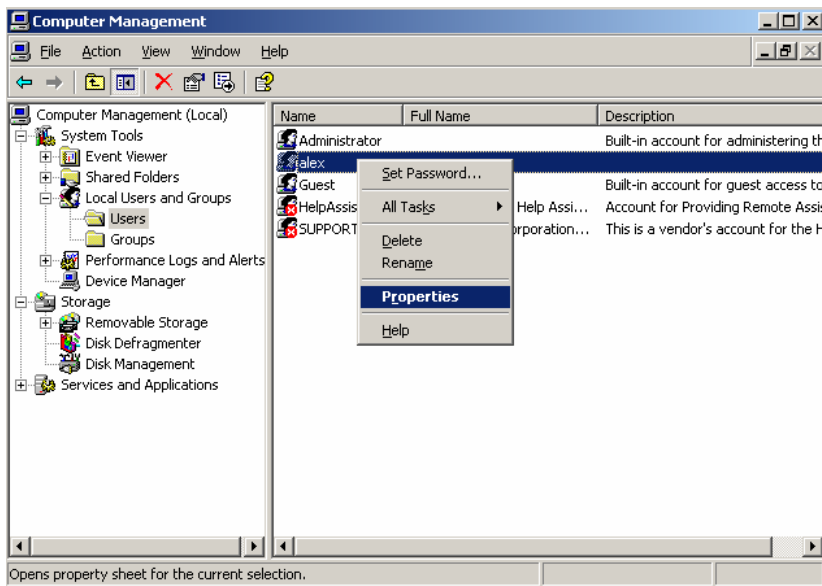


σε αυτήν την καρτέλα βλέπουμε όλους τους τοπικούς χρήστες που υπάρχουν στον συγκεκριμένο υπολογιστή. Για να δημιουργήσουμε νέο χρήστη κάνουμε δεξί κλικ πάνω στο φάκελο users και επιλέγουμε new user .

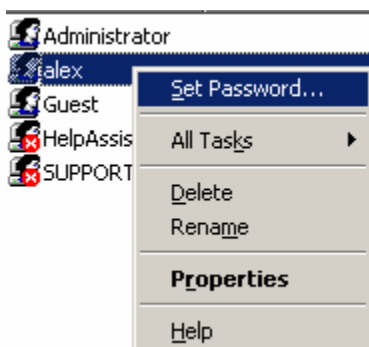


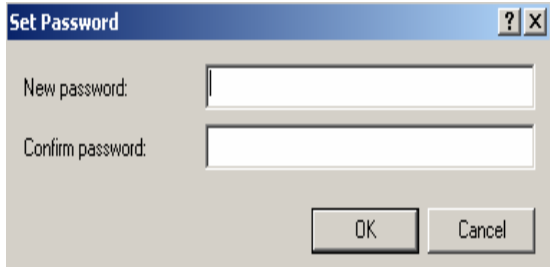


στην επόμενη καρτέλα που εμφανίζεται συμπληρώνουμε τα στοιχεία του νέου μας χρήστη. Με τον ίδιο ακριβώς τρόπο φτιάχνουμε και νέα ομάδα κάνοντας δεξί κλικ πάνω στο φάκελο groups και επιλέγοντας new group . Επιλέγοντας τώρα πάλι τον φάκελο users θα πρέπει στο δεξιό μέρος της οθόνης να εμφανιστεί ο νέος μας χρήστης. Για να επεξεργαστούμε τον χρήστη αυτό, μέλος των administrator κλπ, κλειδωμα χρήστη ) κάνουμε δεξί κλικ πάνω στον χρήστη και επιλέγουμε ιδιότητες (properties).



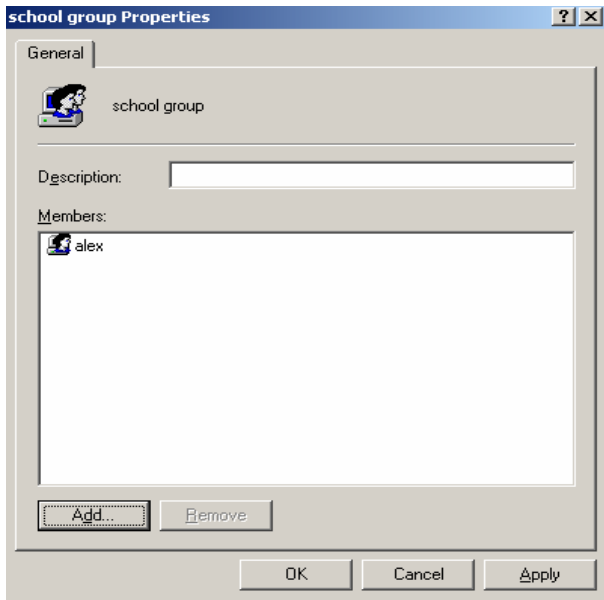
για την αλλαγή κωδικού κάνουμε δεξί κλικ πάνω στον χρήστη και επιλέγουμε ορισμός κωδικού (set password)





A dialog box titled "Set Password" with a question mark icon and a close button (X). It contains two text input fields: "New password:" and "Confirm password:". Below the fields are two buttons: "OK" and "Cancel".

Κάνοντας δεξί κλικ πάνω στην ομάδα που δημιουργήσαμε και επιλέγοντας ιδιότητες (properties) μπορούμε να προσθέσουμε μέλη στην ομάδα αυτήν. (στην νέα καρτέλα που βγαίνει επιλέγω add για να προσθέσω νέα μέλη).



A dialog box titled "school group Properties" with a question mark icon and a close button (X). It has a "General" tab. The "General" tab shows a group icon and the name "school group". Below this is a "Description:" label and an empty text box. Underneath is a "Members:" label and a list box containing one member named "alex" with a small user icon. At the bottom of the list box are "Add..." and "Remove" buttons. At the bottom of the dialog box are "OK", "Cancel", and "Apply" buttons.



## Active Directory

### 1. Active Directory Directory Service.

Η υπηρεσία Active Directory την οποία μας δίνουν τα Win2k με την εγκατάσταση τους είναι ένα εργαλείο διαχείρισης και οργάνωσης του δικτύου μας και συγκεκριμένα της οργάνωσης, διαχείρισης και έλεγχο πρόσβασης (δυνατότητα χρήσης) των πόρων (resources) του δικτύου.

Με τον όρο "πόροι" του δικτύου εννοούμε συνήθως τους users, groups & computers accounts και printers οι οποίοι στη δομή του Active Directory αναπαριστούνται με αντικείμενα (Objects).

Μία από τις σημαντικότερες δυνατότητες που μας παρέχει η υπηρεσία Active Directory είναι η κεντρική διαχείριση των πόρων του δικτύου από κάποιον χρήστη με εξουσιοδότηση ο οποίος καλείται και Administrator του δικτύου.

Συγκεκριμένα ο χρήστης-Administrator δύναται να διαχειρίζεται τους πόρους του δικτύου και από μία μόνον θέση (workstation). Η πληροφορίες σχετικά με την δομή του δικτύου αποθηκεύονται επίσης κεντρικά και αυτό ακριβώς παρέχει την παραπάνω δυνατότητα στον Administrator στο να μπορεί δηλαδή από τον Η/Υ του, όπως λέμε, να έχει πρόσβαση και διαχειριστική δυνατότητα σε όλους τους πόρους του δικτύου.

Από την άλλη πλευρά, των απλών χρηστών, το Active Directory είναι η υπηρεσία δικτύου η οποία δίνει την δυνατότητα χρήσης των πόρων του δικτύου στους χρήστες και τις εφαρμογές που χρησιμοποιούνται με την διαδικασία του Log-On.

### 2. Active Directory Objects.

Το Active Directory αποθηκεύει πληροφορίες σχετικά με τα δικτυακά αντικείμενα που εμπεριέχει. Τα αντικείμενα αυτά (Objects) αντιπροσωπεύουν πόρους του δικτύου μας όπως users, groups, computers και printers. Εκτός από τα παραπάνω Objects υπάρχει ακόμα μία πλειάδα αντικειμένων τα οποία επίσης αποθηκεύονται στην database του Active Directory όπως οι Servers, Domains και Sites.

Ενας Administrator ο οποίος εξ' ορισμού έχει πρόσβαση στην εν' λόγω database μπορεί να διαχειριστεί (manage) κεντρικά όλους τους πόρους του δικτύου του οι οποίοι αναπαρίστανται στο Active Directory με Objects.

Όταν δημιουργείται ένα αντικείμενο οι ιδιότητες του (properties) αποθηκεύονται στο Active Directory. Κατά συνέπεια οι χρήστες μπορούν να βρουν



τη θέση ενός αντικειμένου πχ ενός εκτυπωτή, ψάχνοντας μέσα στο Active Directory για αντικείμενα που ικανοποιούν τις συγκεκριμένες ιδιότητες (properties).

Υπάρχει και μία κατηγορία ακόμα αντικειμένων των οποίων ο ρόλος είναι να εμπεριέχουν άλλα αντικείμενα. Αναφερόμαστε στα Objects : Domains, Containers και Organizational Units τα οποία μπορούν να οργανωθούν είτε ιεραρχικά (hierarchy) είτε σε δενδροειδή (forest) μορφή. Εν συνεχεία Objects όπως users, groups, printers και shared folders – files, τοποθετούνται μέσα σε Domain, Container και Organizational Unit, σε συνάρτηση με τον τρόπο που θέλουμε να τα διαχειριστούμε.



### 3. User Accounts.

Με τον όρο User Account εννοούμε την καταχώρηση (δήλωση) ενός προσώπου-χρήστη ενός Η/Υ ή ενός δικτύου Η/Υ στην λίστα των εξουσιοδοτημένων χρηστών του συστήματος, έτσι ώστε μέσω μίας διαδικασίας που ονομάζετε Log-On να μπορεί να χρησιμοποιήσει τους πόρους του Η/Υ ή του δικτύου των Η/Υ.

Η διαδικασία Log-On είναι η διαδικασία κατά την οποία δηλώνετε το user name και το password στο σύστημα. Στη συνέχεια το σύστημα ελέγχει την ύπαρξη του εν' λόγω χρήστη στη λίστα χρηστών (users accounts) και αναλόγως εξουσιοδοτεί (authentication) τον χρήστη να χρησιμοποιήσει τους πόρους του δικτύου.

Υπάρχουν τριών ειδών user accounts.

#### I. Local User Account.

Είναι ο χρήστης ο οποίος με την διαδικασία Log-On δίνετε να κάνει χρήση των πόρων του Η/Υ στον οποίο κάνει Log-On (ζητά εξουσιοδότηση).

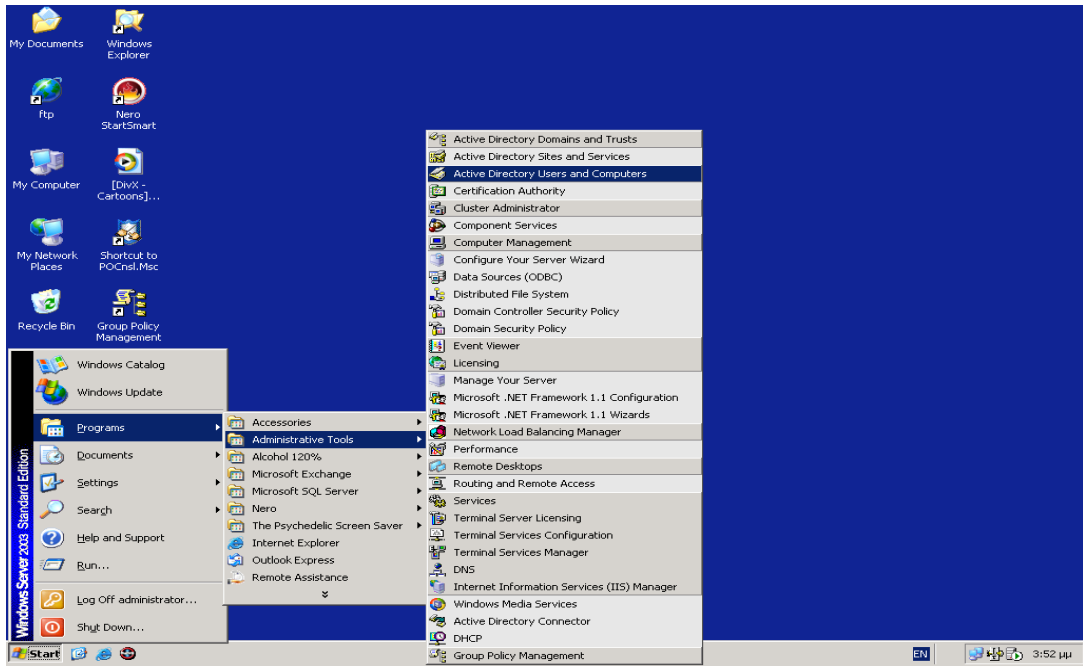
#### II. Domain User Account.

Είναι ο χρήστης ο οποίος με την διαδικασία Log-On δίνετε να κάνει χρήση των πόρων του Domain στο οποίο κάνει Log-On (ζητά εξουσιοδότηση).

#### III. Built-in User Account.

Είναι ο χρήστης ο οποίος με την διαδικασία Log-On δίνετε να αποκτήσει διαχειριστικές δυνατότητες ή να αποκτήσει πρόσβαση στους πόρους του δικτύου πρόσκαιρα.

Στο Active Directory τα User Accounts αναπαριστώνται με Objects και βρίσκονται μέσα στο Active Directory User and Computers.





Κατά την διαδικασία Log-On χρειάζεται να δηλωθεί ένα όνομα (name) και ένα συνθηματικό (password). Επίσης στα Win2k υπάρχει ένα User Logon Name και ένα pre-Win2k User Logon Name το οποίο είναι το SAM (Security Account Name).

Κατά τη δημιουργία ενός User Account πρέπει να οριστεί αφ' ενός το user logon name prefix όπως επίσης και να επιλεγθεί το user principal name suffix (UPN). Τέλος όταν δημιουργούμε ένα νέο user account θα πρέπει να λάβουμε υπόψη μας τους κανόνες μοναδικότητας του.

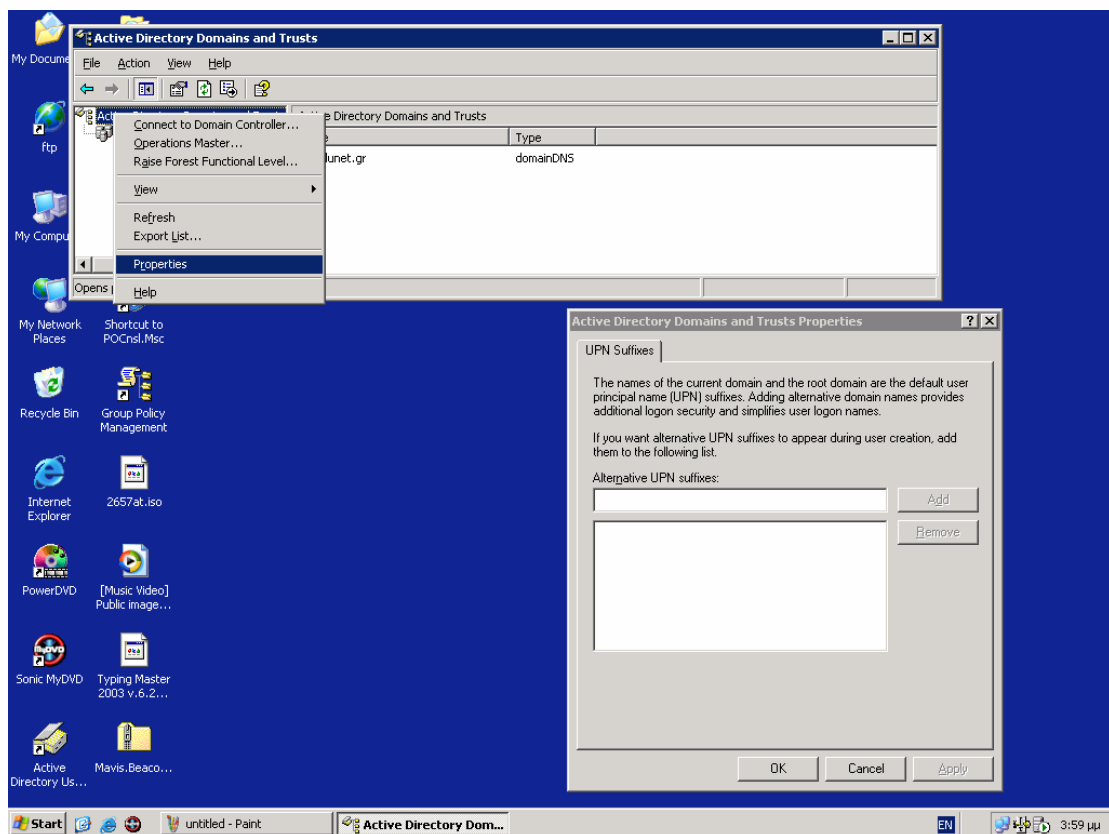
Σ' ένα δίκτυο Win2k ένας χρήστης μπορεί να κάνει Log-On είτε χρησιμοποιώντας το User Principal Name (UPN) είτε το User Logon Name (για pre-Win2k).

Το UPN, το οποίο επίσης λέγεται και απλώς user logon name, αποτελείται από δύο κομμάτια το UPN prefix και το UPN suffix.

Πχ. kostas@edunet.gr  
Prefix - S u f f i x

Εξ' ορισμού (by default) το UPN suffix είναι το όνομα του root domain του δικτύου. Μπορούμε εάν θέλουμε να φτιάξουμε επιπλέον suffixes χρησιμοποιώντας άλλα Domain του δικτύου (κατά την κρίση του Administrator).

Παράδειγμα δημιουργίας UPN suffix :









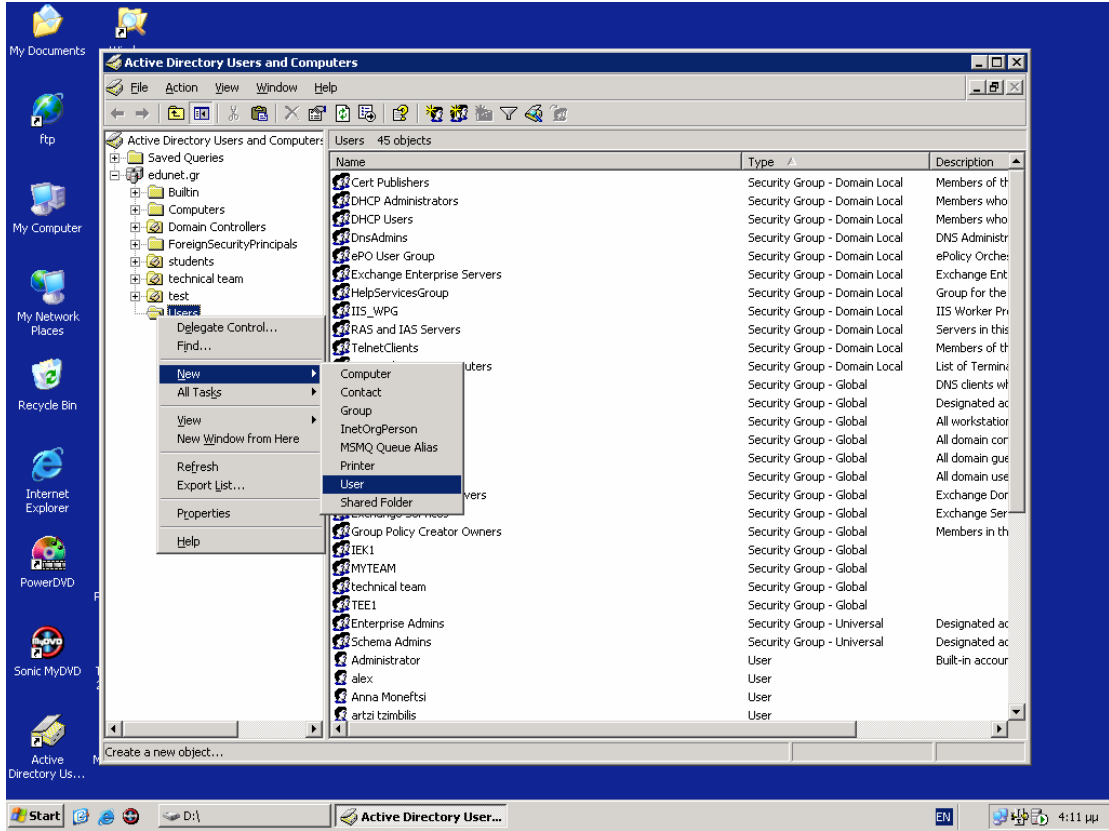
Το User Logon Name (pre-Win2k) χρησιμοποιείται από χρήστες οι οποίοι θέλουν να κάνουν logon σ' ένα δίκτυο Win2k από ένα σταθμό ο οποίος έχει Λειτουργικό Σύστημα pre-Win2k. Λαμβάνοντας υπόψη το προηγούμενο παράδειγμα το User Logon Name θα ήταν το "kostas". Κατά την διαδικασία logon ενός pre-Win2k σταθμού εργασίας ο χρήστης θα πρέπει να δηλώσει και το Domain στο οποίο θέλει να κάνει logon. Ένα παράδειγμα logon σ' ένα τέτοιο σύστημα θα είχε την εξής σύνταξη :

Πχ Edunet\kostas

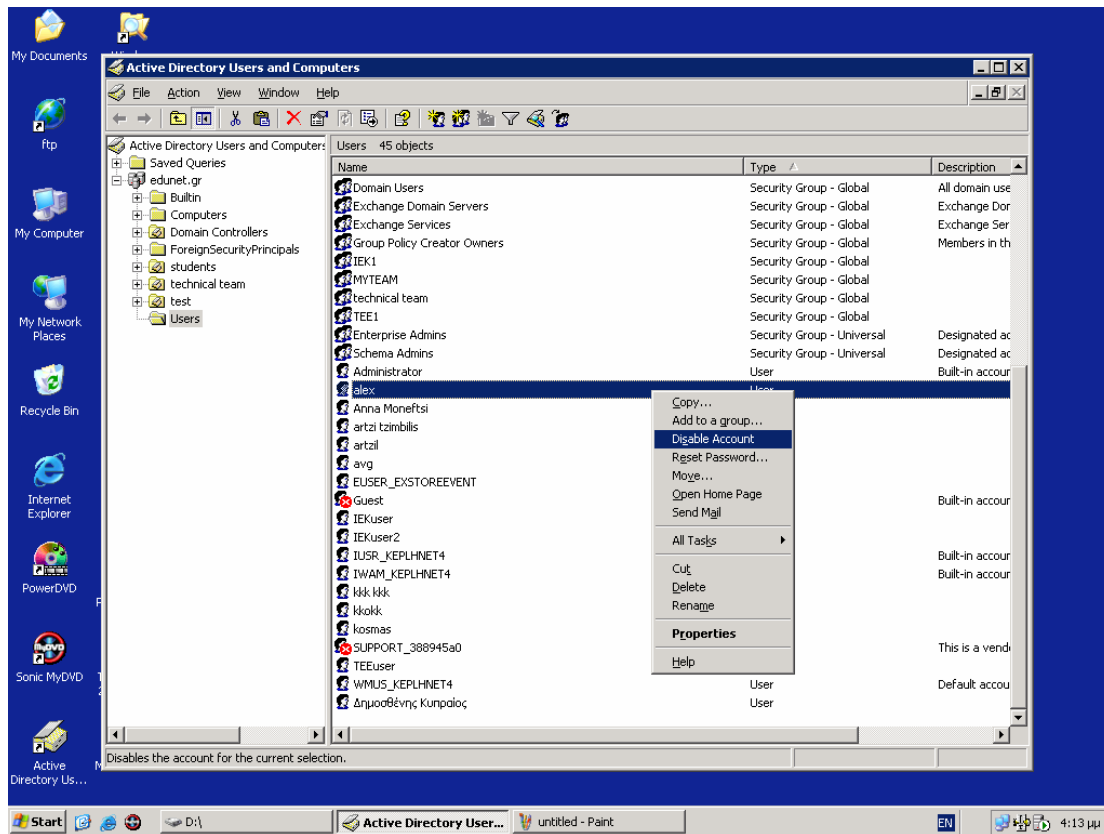
Οι κανόνες μοναδικότητας που πρέπει να λαμβάνουμε υπόψη μας κατά την δημιουργία ενός User Logon Name στο Active Directory ενός Domain είναι οι εξής:

- I. Το full name πρέπει να είναι μοναδικό μέσα στο container που δημιουργούμε τον χρήστη.
- II. Το UPN πρέπει να είναι μοναδικό μέσα στο forest.
- III. Το user logon name (pre-Win2k) πρέπει να είναι μοναδικό μέσα στο Domain.

Παράδειγμα δημιουργίας χρήστη στο Active Directory :



Διαχείριση χρηστών από το Active Directory User and Computers.



- **Disabling & Enabling User Accounts.**
- **Resetting Passwords.**
- **Delete.**
- **Rename.**
- **Properties.**



## 4. Groups.

Με τον όρο Group εννοούμε ένα σύνολο από user accounts.

Τα Groups χρησιμοποιούνται για να διαχειριζόμαστε ποιο έξυπνα (ποιο εύκολα) τα user accounts ως προς την εξουσιοδότηση τους για την χρήση των πόρων του δικτύου. Με την χρήση των groups πετυχαίνουμε καλύτερη συντήρηση και διαχείριση του συνολικού δικτύου. Μπορούμε επίσης να τοποθετήσουμε ένα group μέσα σε κάποιο άλλο για ακόμα ευκολότερη διαχείριση. Έτσι δίνοντας μία φορά δικαιώματα σε κάποιο group αποφεύγουμε να επαναλάβουμε την ίδια διαδικασία εκχώρησης δικαιωμάτων για κάθε ένα χρήστη που ανήκει στο group.

Υπάρχουν δύο ειδών group στο Active Directory. Τα **Security Groups** και τα **Distribution Groups**. Και τα δύο παραπάνω είδη των group μπορούμε να πούμε ότι υποδιαιρούνται σε τρεις ακόμα κατηγορίες (group scope) τις εξής :

- I. **Domain Local Group.**
- II. **Global Group**
- III. **Universal Group.**

Οι Users μπορούν να ανήκουν σε παραπάνω από ένα Group.

Security Groups χρησιμοποιούμε για να εκχωρήσουμε δικαιώματα σε group χρηστών ή H/Y.

Distribution Groups χρησιμοποιούμε για εργασίες mailing, Exchange και όχι για security σκοπούς.

Και τα δύο είδη των groups έχουν ιδιότητες (scope) με βάση τις οποίες προσδιορίζετε ποιος μπορεί να είναι μέλος σ' αυτό το group και που μπορεί να χρησιμοποιηθεί αυτό το group μέσα στο δίκτυο.

Ένας έξυπνος τρόπος διαχείρισης των groups είναι το **Nesting** δηλαδή η προσθήκη group μέσα σε άλλο group. Μ' αυτό τον τρόπο ιεραρχούμε τα δικαιώματα του group το οποίο είναι μέλος ενός άλλου group και απλοποιούμε την παραχώρηση δικαιωμάτων.

Το Nesting δεν μπορεί να χρησιμοποιηθεί σε mixed-domain mode δίκτυα (Win2k & WinNT Domain Controllers).

Αναφορικά με τα group scope χρησιμοποιούμε :

- I. **Domain Local Group** για να εκχωρήσουμε δικαιώματα χρήσης πόρων δικτύου οι οποίοι βρίσκονται στο ίδιο Domain που δημιουργούμε το group.
- II. **Global Group** για να εκχωρήσουμε δικαιώματα χρήσης πόρων δικτύου για χρήστες που έχουν κοινές απαιτήσεις στην χρήση των πόρων λόγω του ότι συνήθως κάνουν κοινές εργασίες.
- III. **Universal Group** για να καταχωρήσουμε global groups μέσα σ' αυτά και να μπορέσουμε τελικώς να δώσουμε δικαιώματα



χρήσης πόρων που ανήκουν σε διαφορετικά Domain. Απαιτείτε να είμαστε σε native domain mode (Only Win2k Domain Controllers).

Σ' ένα single domain δίκτυο έχουμε δυνατότητα χρήσης μόνο των Domain Local & Global Groups.

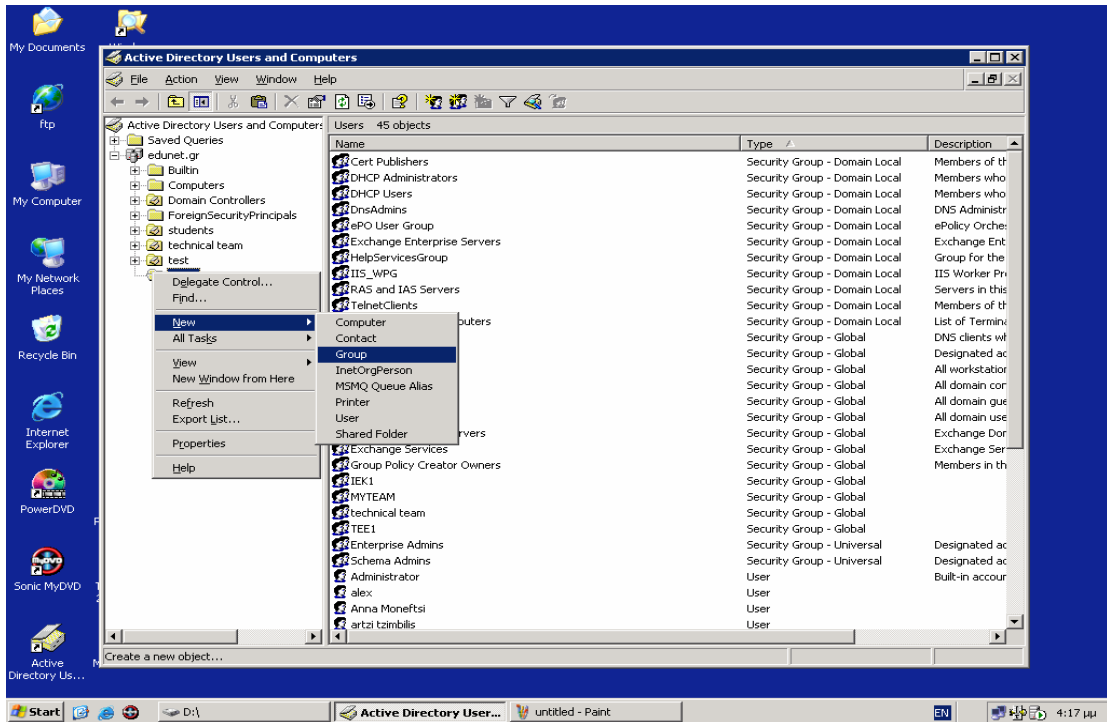
Η συνήθης μεθοδολογία χρήσης Local & Global Groups είναι η εξής :

- |                      |  |
|----------------------|--|
| 1. A (Add)           | Δημιουργία User Accounts.                          |
| 2. G (Global)        | Προσθήκη των User Accounts σε Global Group.        |
| 3. DL (Domain Local) | Προσθήκη των Global Groups σε Domain Local Groups. |
| 4. P (Permission)    | Εκχώρηση δικαιωμάτων στο Domain Local Group.       |

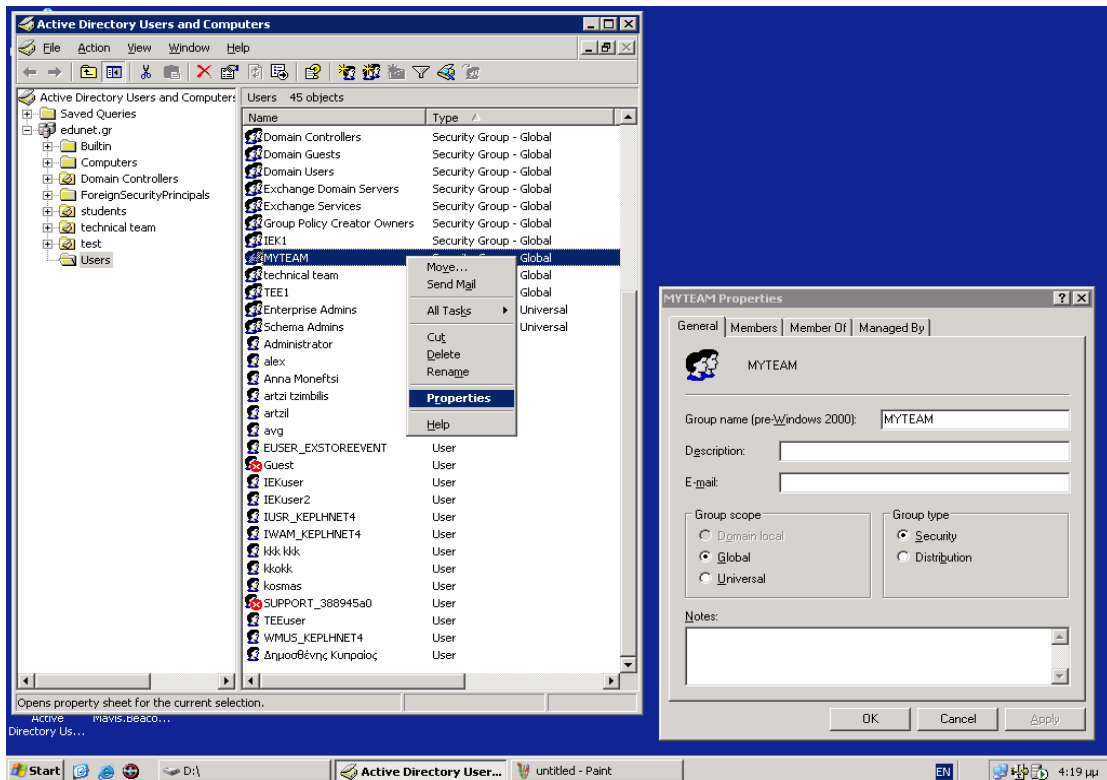
Μία παραλλαγή της παραπάνω μεθοδολογίας είναι και το Group Nesting.

- |                      |  |
|----------------------|--|
| 1. A (Add)           | Δημιουργία User Accounts.                                |
| 2. G (Global)        | Προσθήκη των User Accounts σε Global Group.              |
| 3. G (Global)        | ---- NESTING ----  |
| 4. DL (Domain Local) | Προσθήκη των Global Groups σε Domain Local<br>i. Groups. |
| 5. P (Permission)    | Εκχώρηση δικαιωμάτων στο Domain Local<br>i. Group.       |

Δημιουργία Groups στο Active Directory User and Computers.



Διαχείριση Groups από το Active Directory User and Computers.



User Accounts Member of a Security Group.



The screenshot shows the Active Directory Users and Computers console. The left pane shows the tree structure with 'edunet.gr' expanded to 'Users'. The right pane lists 45 objects, including various security groups and users. The 'MYTEAM' group is selected. A 'MYTEAM Properties' dialog box is open, showing the 'Members' tab. The members list contains three entries:

Name	Active Directory Folder
artzi tzimblis	edunet.gr/Users
artzi	edunet.gr/Users
kkokk	edunet.gr/Users

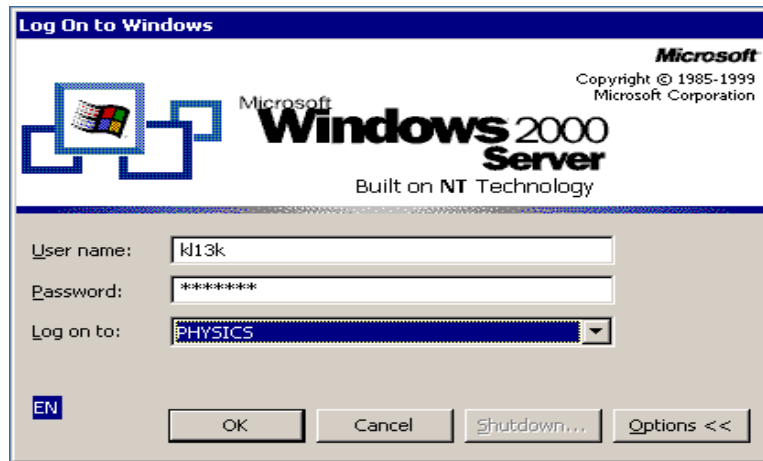
The dialog box also has 'Add...' and 'Remove' buttons, and 'OK', 'Cancel', and 'Apply' buttons at the bottom.



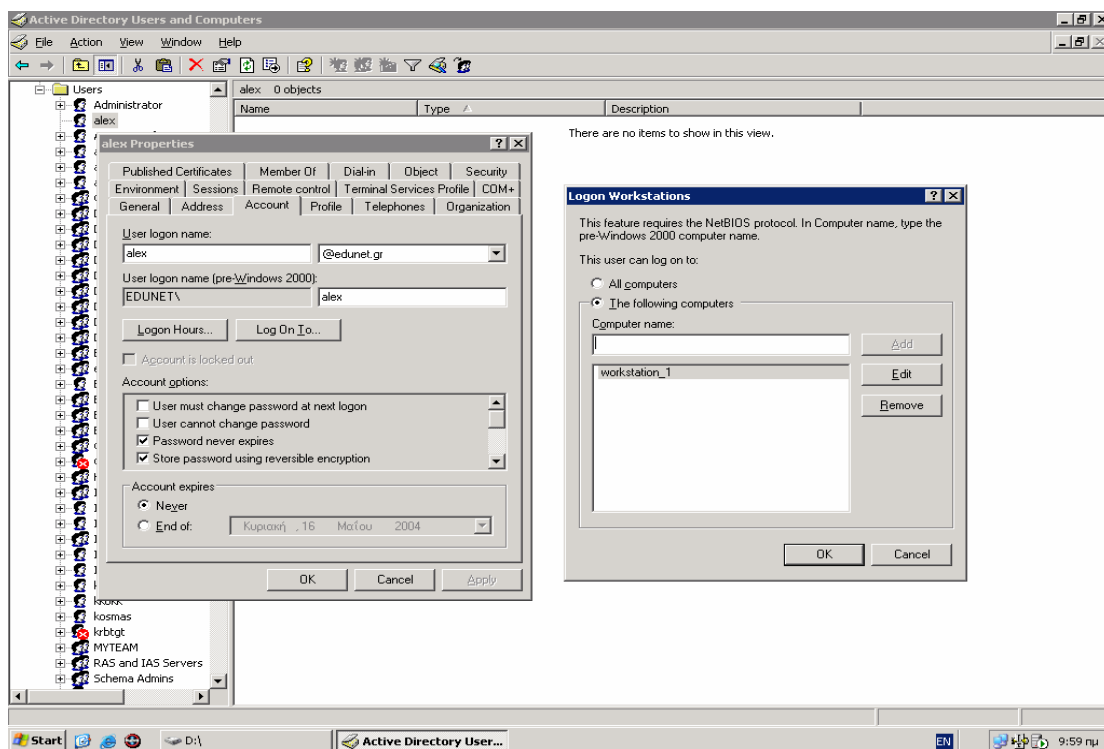
## Troubleshooting.

- Κατά την διαδικασία Logon του χρήστη “kostas” δεν κάνει Logon. Πιθανές αιτίες και ενέργειες επίλυσης.

-Λάθος εισαγωγή PSW, πιθανός σε άλλη γλώσσα ή με κεφαλαίους χαρακτήρες. Εισαγωγή PSW εκ νέου.



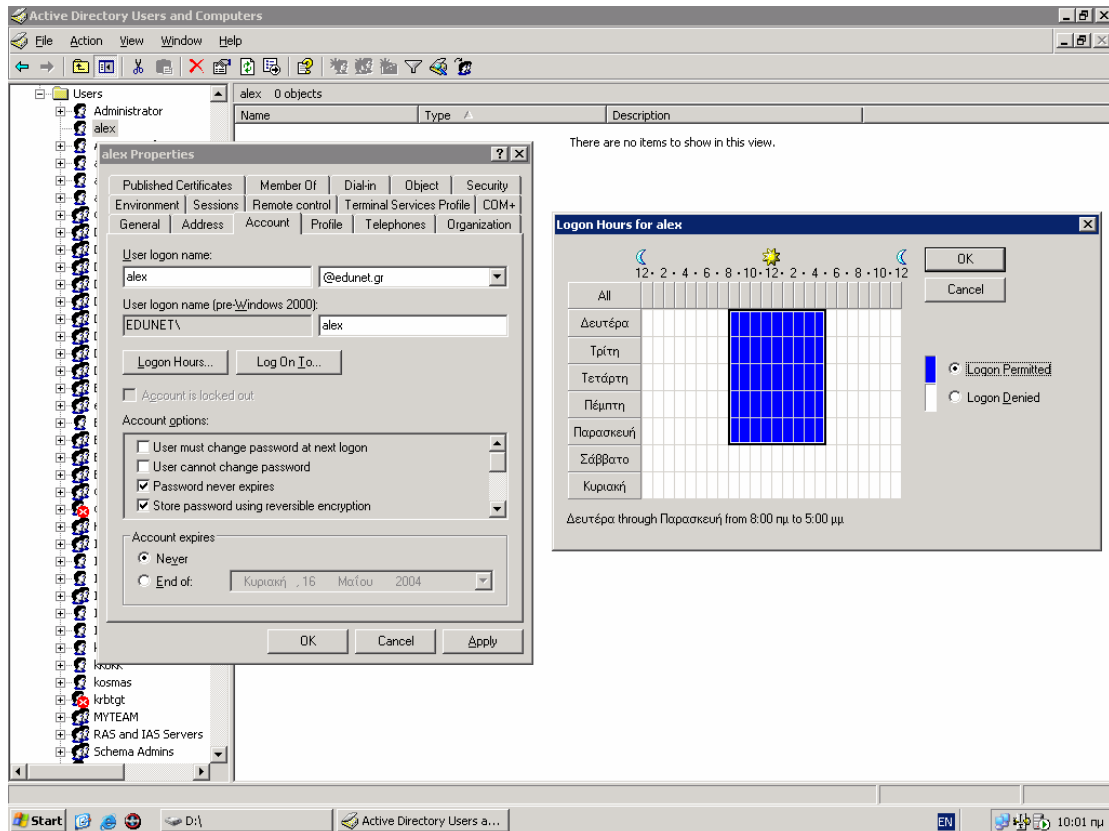
- Κλείδωμα user με computer. Properties user – καρτέλα “access” – Logon To.







- Εξουσιοδότηση user για Logon σε συγκεκριμένες ώρες και μέρες της εβδομάδας. Properties user – καρτέλα “access” – Logon Hours.





## Organization Unit's

### Τί είναι το OU(organizational unit);

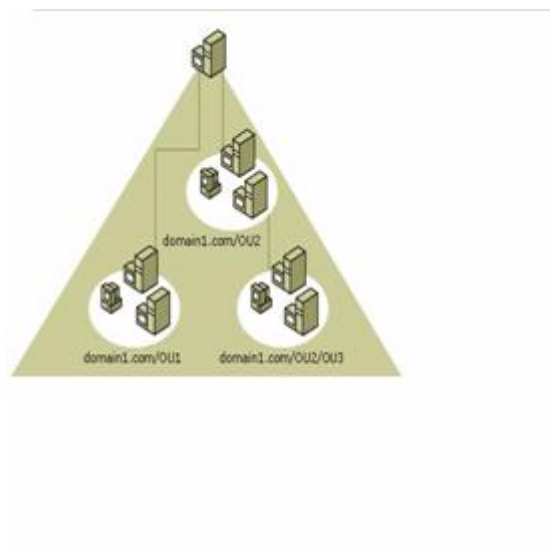
Ένα ιδιαίτερα χρήσιμο είδος αντικειμένου του AD(Active Directory) το οποίο περιέχεται στο Domain είναι το OU(Organization Unit).

Τα Ου's είναι μέρη του AD(Active Directory) στα οποία μπορούμε να τοποθετήσουμε Users(χρήστες), Groups (ομάδες), Computers (υπολογιστές), Printers (εκτυπωτές) και άλλα ΟΥ'S. Ένα ΟΥ δεν μπορεί να περιέχει ΟΥ'S από άλλα Domain.

### Γιατί να χρησιμοποιούμε ΟΥ;

Ένα ΟΥ είναι η μικρότερη μονάδα πάνω στην οποία μπορούν να εφαρμοστούν ρυθμίσεις GP(Group Policy) ή να αποδοθεί(delegate) administrative authority σε ένα χρήστη(user) ή σε μια ομάδα(group).

Χρησιμοποιώντας ΟΥ'S μπορούμε να δημιουργήσουμε υποομάδες μέσα σε ένα Domain τα περιεχόμενα των οποίων(users,groups,printers etc.) θα αναπαριστούν ιεραρχικά την λογική δομή του οργανισμού μας(π.χ δίκτυο σχολικού εργαστηρίου). Έπειτα μπορούμε να διαχειριστούμε εύκολα τις ρυθμίσεις των λογαριασμών και των άλλων resources με βάση αυτό το οργανωτικό μοντέλο.



Όπως φαίνεται και στο σχήμα τα ΟΥ's μπορούν να περιέχουν και άλλα ΟΥ's. Η δομή των υποσυνόλων (ΟΥ's) μπορεί να επεκταθεί όσο είναι απαραίτητο για να εξυπηρετεί το δίκτυο μας μέσα στο domain. Χρησιμοποιώντας ΟΥ's μπορούμε να μειώσουμε τον αριθμό των domains που απαιτεί το δίκτυο μας. Όταν οργανώνουμε το δίκτυο μας με τη βοήθεια των ΟΥ's μπορούμε πολύ πιο εύκολα να αποδώσουμε δικαιώματα(delegate control) σε συγκεκριμένους χρήστες(users) ή ομάδες(groups) οι οποίοι θα μπορούν να διαχειρίζονται και εκείνοι το συγκεκριμένο ΟΥ.



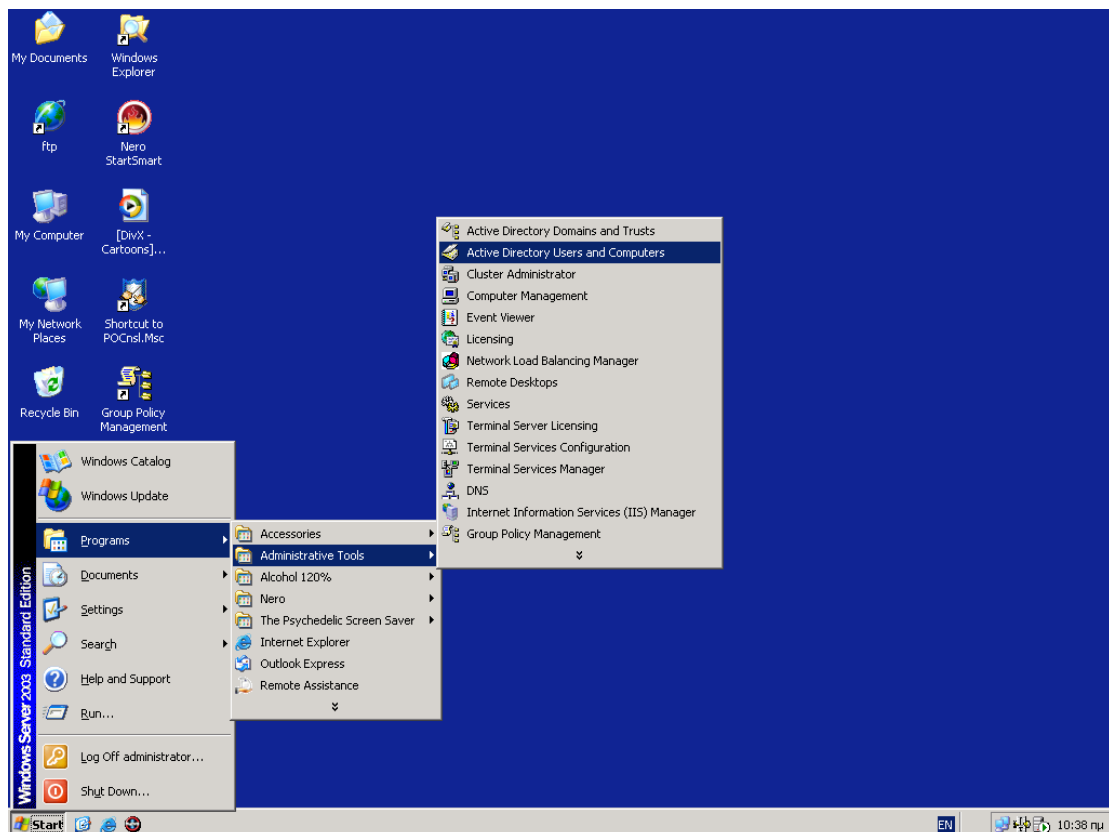
Επίσης με τη μέθοδο αυτή μπορούμε να ασφαλίσουμε το δίκτυο μας πιο αποτελεσματικά σε περίπτωση τυχαίας ή επιτιδευμένης βλάβης(δικτυακής φύσης) περιορίζοντας τα μέλη του group των administrators.

Για να αποφασίσουμε τι OU's θα χρησιμοποιήσουμε πρέπει να λάβουμε υπ'οψιν μας τη δομή του δικτύου μας.

Για παράδειγμα στον Server του εργαστηρίου μας μπορούμε να φτιάξουμε OUs για κάθε τμήμα που χρησιμοποιεί το εργαστήριο ή ακόμα OUs για κάθε ειδικότητα που χρησιμοποιεί το εργαστήριο. (άλλα δικαιώματα θα έχουν οι χρήστες προγραμμάτων Cad και άλλα οι απλοί χρήστες Ιντερνετ.)

## Πώς μπορούμε να δημιουργήσουμε ένα OU:

1. Συνδεόμαστε σαν διαχειριστές administrator.
2. Πάμε Start→Programs→Administrative Tools→Active Directory Users And Computers.

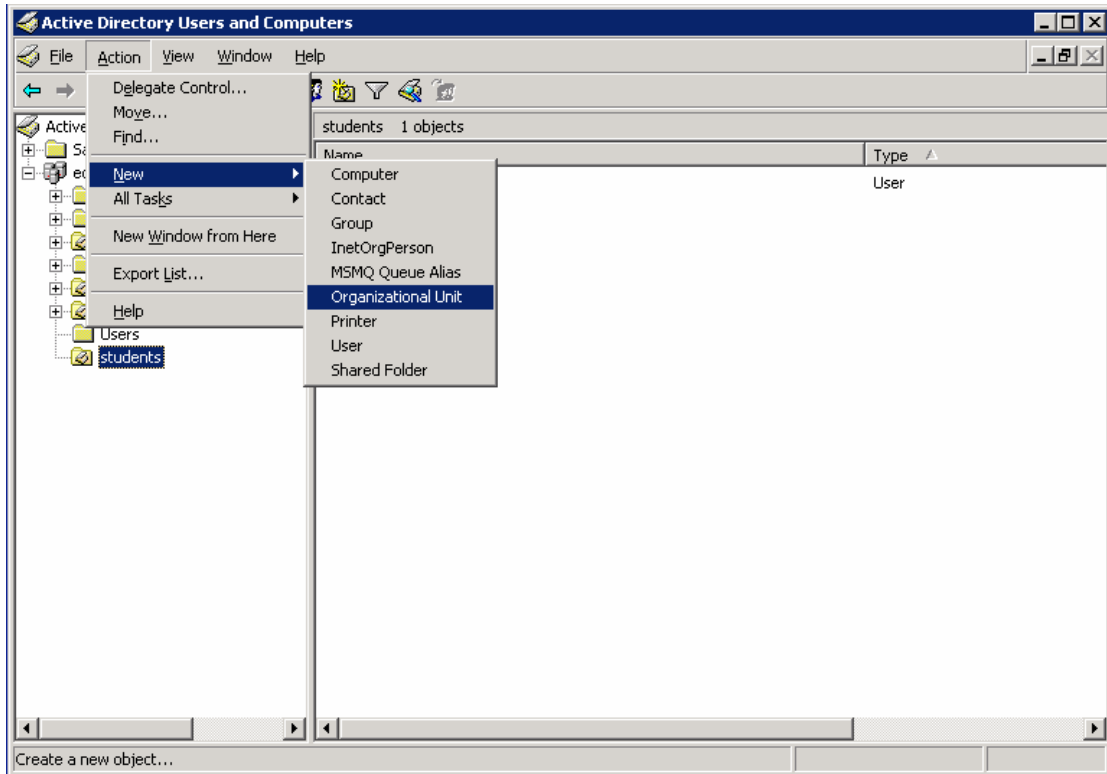


3. Κάνουμε ένα από τα εξής:

- Δεξί κλικ στο αντικείμενο του domain ή στο OU μέσα στο οποίο θέλουμε να δημιουργήσουμε άλλα OU's,πάμε Add και μετά Organizational Unit.



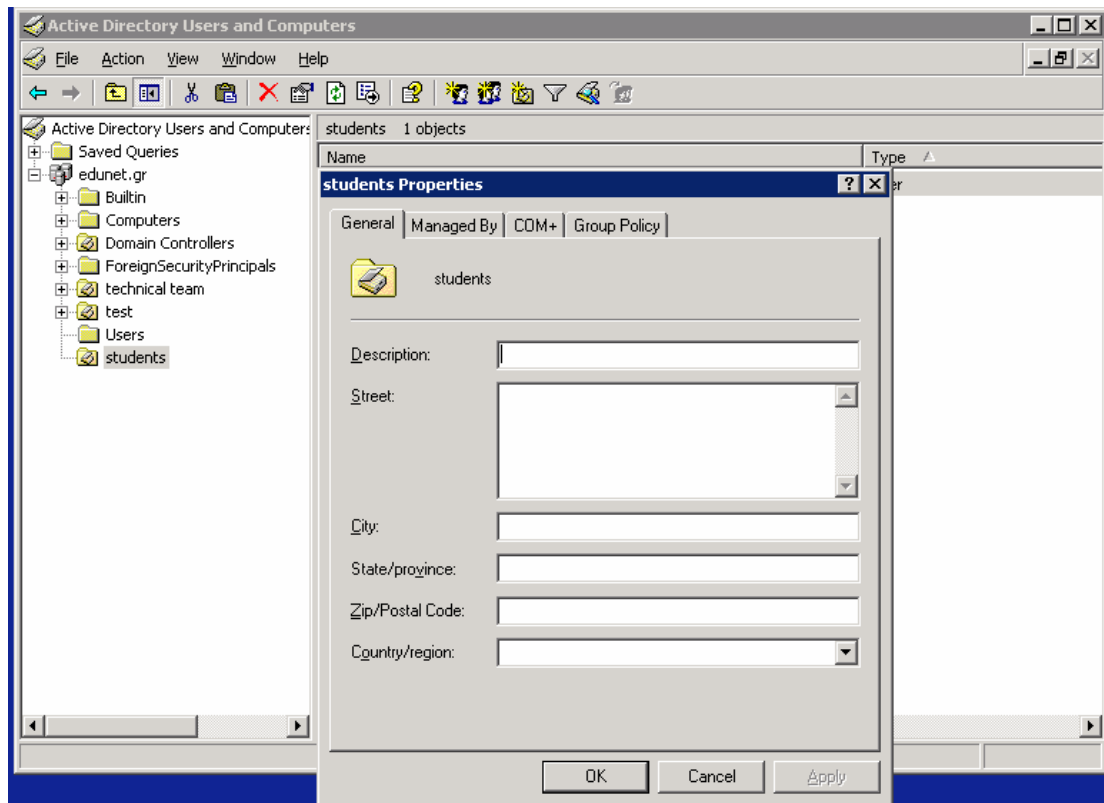
- Πάμε Create New Organizational Unit.  
Στο μενού Action→New→Organizational Unit.



4. Στο πεδίο ονόματος βάζουμε το όνομα που θα χαρακτηρίζει το καινούργιο αντικείμενο και πατάμε OK. Ένα εικονίδιο με το κατάλληλο όνομα δημιουργείται και εισάγεται στη λίστα. Τώρα μπορούμε να προσθέσουμε και άλλα αντικείμενα στο OU όπως χρήστες, υπολογιστές, ομάδες και άλλα OU's.

### Πώς μπορούμε να αλλάξουμε τα χαρακτηριστικά ενός OU;

1. Πάμε Start→Programs→Administrative Tools→Active Directory Users And Computers
2. Κάνουμε κλικ πάνω στο domain επεκτείνοντας τη λίστα.
3. Έπειτα πάμε στο OU που μας ενδιαφέρει και Properties στο Action Menu.
4. Αφού επιλέξουμε την καρτέλα που μας ενδιαφέρει βάζουμε τις κατάλληλες τιμές.





Κοινή Χρήση Φακέλων (Shared Folders) .....	67
Χρήση Κοινόχρηστων Φακέλων .....	67
Προαπαιτούμενα για Κοινή Χρήση .....	68
Μοιράζοντας έναν Φάκελο .....	68
Προσωρινή αποθήκευση (Caching) – Offline Files .....	70
Δικαιώματα Κοινόχρηστων Φακέλων .....	71
Εκχώρηση δικαιωμάτων Κοινόχρηστου Φακέλου .....	74
Τροποποίηση ρυθμίσεων Κοινόχρηστου Φακέλου .....	75
Κοινόχρηστοι Φάκελοι Διαχείρισης .....	76
Ασφάλεια .....	77
Δικαιώματα NTFS .....	77
Πολλαπλά Δικαιώματα NTFS .....	78
Μεταβίβαση δικαιωμάτων NTFS .....	80
Αντιγραφή και Μετακίνηση Αρχείων και Φακέλων .....	81
Εφαρμογή δικαιωμάτων NTFS .....	82
Εκχώρηση δικαιωμάτων NTFS .....	83
Ρύθμιση Μεταβίβασης Δικαιωμάτων .....	85
Συνιστώμενες Πρακτικές .....	86
Συνδυασμός δικαιωμάτων NTFS και Κοινής Χρήσης .....	87
Κοινή Χρήση Φακέλων (Shared Folders) .. <b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>	
Χρήση Κοινόχρηστων Φακέλων .....	<b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>
Προαπαιτούμενα για Κοινή Χρήση .....	<b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>
Μοιράζοντας έναν Φάκελο .....	<b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>
Προσωρινή αποθήκευση (Caching) – Offline Files .....	<b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>
Δικαιώματα Κοινόχρηστων Φακέλων ....	<b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>
Εκχώρηση δικαιωμάτων Κοινόχρηστου Φακέλου .....	<b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>
Τροποποίηση ρυθμίσεων Κοινόχρηστου Φακέλου .....	<b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>
Κοινόχρηστοι Φάκελοι Διαχείρισης .....	<b>Σφάλμα! Δεν έχει οριστεί σελιδοδείκτης.</b>





## Κοινή Χρήση Φακέλων (Shared Folders)

### Χρήση Κοινόχρηστων Φακέλων



Χρησιμοποιούμε τους Κοινόχρηστους Φακέλους για να δώσουμε στους χρήστες την δυνατότητα πρόσβασης σε φακέλους, και στα αρχεία τα οποία περιέχουν, που δεν βρίσκονται στον υπολογιστή τον οποίο χρησιμοποιούν, αλλά σε κάποιον άλλο, μέσω του δικτύου.

Με τους Κοινόχρηστους Φακέλους:

- Διευκολύνουμε τους χρήστες παρέχοντάς τους ένα κεντρικό σημείο μέσω του οποίου έχουν πρόσβαση σε αρχεία που χρησιμοποιούν.
- Διευκολύνουμε τον διαχειριστή του συστήματος στην δημιουργία αντιγράφων ασφαλείας αυτών των αρχείων.
- Απλοποιείται η διαχείριση με τους Κοινόχρηστους Φακέλους Εφαρμογών, αφού μπορούμε να εγκαταστήσουμε και να συντηρούμε μια εφαρμογή σε έναν Server αντί να κάνουμε το ίδιο σε όλους τους σταθμούς εργασίας.





## Προαπαιτούμενα για Κοινή Χρήση

Οι προϋποθέσεις για να μοιράσουμε έναν φάκελο καθορίζονται από τα εξής:

- i. Εάν οι κοινοί φάκελοι βρίσκονται σε υπολογιστή Τομέα (Domain) ή σε ομάδα εργασίας (Workgroup)
- ii. Ο τύπος λειτουργικού συστήματος του υπολογιστή στον οποίο βρίσκεται ο κοινόχρηστος φάκελος

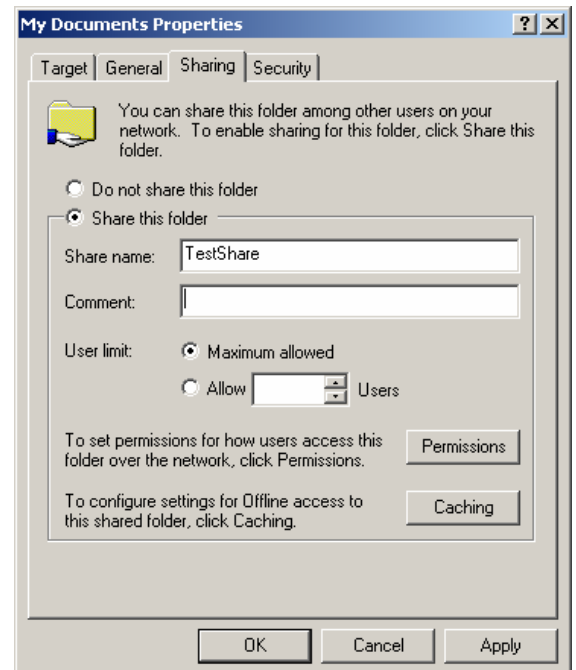
Ο παρακάτω πίνακας περιγράφει ποιοι μπορούν να μοιράζουν φακέλους

Για να “μοιράσετε” φακέλους που βρίσκονται σε	Πρέπει να είστε μέλος
Windows 2000 Domain Controller	<b>Administrators ή Server Operators</b>
Windows 2000 Stand-alone ή Member Server	<b>Administrators ή Power Users</b>
Πελάτη-Υπολογιστή με Windows 2000 Professional	<b>Administrators ή Power Users</b>

## Μοιράζοντας έναν Φάκελο

Όταν μοιράζουμε έναν φάκελο του δίνουμε ένα όνομα με το οποίο θα εμφανίζεται ως κοινόχρηστος, μπορούμε να προσθέσουμε σχόλια που θα περιγράφουν τον φάκελο και τα περιεχόμενά του, να περιορίσουμε τον αριθμό των χρηστών που μπορούν να συνδεθούν ταυτόχρονα με αυτόν, και να εκχωρήσουμε δικαιώματα.

Για να δημιουργήσουμε έναν Κοινόχρηστο Φάκελο, κάνουμε δεξί κλικ στον φάκελο και επιλέγουμε Κοινή Χρήση ( ή Sharing αν το λειτουργικό σύστημα είναι στα Αγγλικά). Στην καρτέλα Κοινή Χρήση ρυθμίζουμε τις επιλογές που περιγράφονται στον ακόλουθο πίνακα:



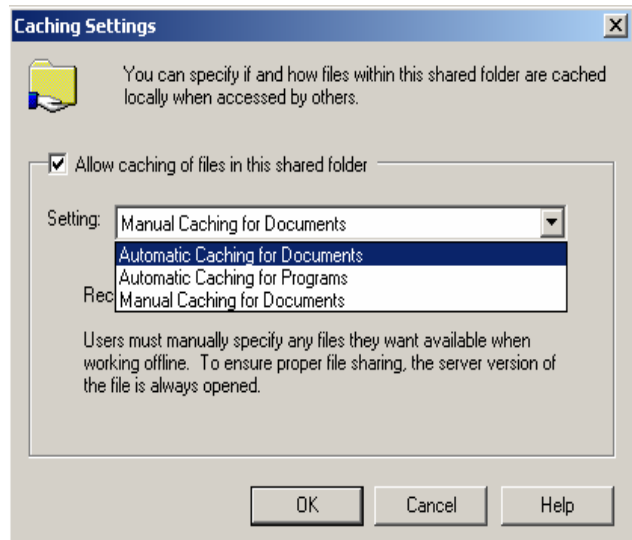


Επιλογή	Περιγραφή
Share this folder Κοινή χρήση αυτού του φακέλου	Το επιλέγουμε για να μοιράσουμε τον φάκελο
Share name Κοινόχρηστο στοιχείο	Εισάγουμε το όνομα με το οποίο θα βλέπουν οι χρήστες τον φάκελο. Ως προεπιλογή είναι το όνομα του φακέλου.
Comment Σχόλιο	Προαιρετική περιγραφή του κοινόχρηστου φακέλου.
User Limit Όριο χρηστών	Η επιλογή Maximum Allowed (Μέγιστο όριο) επιτρέπει στον μέγιστο αριθμό χρηστών να συνδεθούν ταυτόχρονα στον κοινόχρηστο φάκελο. Τα Windows 2000 Professional υποστηρίζουν μέχρι 10 συνδέσεις ενώ τα Windows 2000 Server υποστηρίζουν τόσες συνδέσεις όσες οι άδειες χρήσης του Server. Η επιλογή Allow ( Έως) περιορίζει τον αριθμό των χρηστών που μπορούν να συνδεθούν ταυτόχρονα.
Permissions Δικαιώματα	Κάντε κλικ για να ορίσετε δικαιώματα κοινής χρήσης που ισχύουν μόνο όταν ο φάκελος προσεγγίζεται μέσω δικτύου. Από προεπιλογή <b>εκχωρούνται πλήρη δικαιώματα στην ομάδα Everyone</b> για όλους τους καινούργιους κοινόχρηστους φακέλους
Caching Προσωρινή αποθήκευση	Με την επιλογή αυτή μπορούμε να επιτρέψουμε στους χρήστες να αποθηκεύουν τοπικά τα αρχεία του κοινόχρηστου φακέλου, ώστε να είναι διαθέσιμα όταν δεν υπάρχει σύνδεση (Offline Files)
New Share Νέο κοινόχρηστο στοιχείο	Μπορούμε να μοιράσουμε τον ίδιο φάκελο πολλές φορές με άλλο όνομα. Αυτό μας δίνει την δυνατότητα να συγχωνεύσουμε πολλούς κοινόχρηστους φακέλους σε έναν, επιτρέποντας ταυτόχρονα στους χρήστες να χρησιμοποιούν το ίδιο κοινόχρηστο όνομα που χρησιμοποιούσαν πριν την συγχώνευση.



## Προσωρινή αποθήκευση (Caching) – Offline Files

Επιλέγοντας Caching (Προσωρινή αποθήκευση) από την καρτέλα Sharing ( Κοινή χρήση) ανοίγει το παράθυρο Caching Settings (Ρυθμίσεις μνήμης Cache) όπου μπορούμε να ορίσουμε αν ο κοινόχρηστος φάκελος θα είναι διαθέσιμος offline (τσεκάροντας το Allow caching of files in this shared folder). Έχουμε τρεις επιλογές για να ρυθμίσουμε το πώς θα εφαρμοστεί αυτή η δυνατότητα:



- i. **Automating Caching for Documents** (Αυτόματη προσωρινή αποθήκευση εγγράφων). Τα αρχεία που έχουν ανοιχτεί λαμβάνονται αυτόματα τοπικά και είναι διαθέσιμα κατά την εργασία χωρίς σύνδεση (offline). Παλαιότερα αρχεία διαγράφονται τοπικά ώστε να ελευθερωθεί χώρος για αρχεία νεώτερα ( πιο πρόσφατης πρόσβασης). Για να διασφαλιστεί η σωστή κοινή χρήση των αρχείων ανοίγεται πάντα η έκδοση του διακομιστή του αρχείου. Συνιστάται για φακέλους οι οποίοι περιέχουν έγγραφα χρήστη.
- ii. **Automating Caching for Programs** (Αυτόματη προσωρινή αποθήκευση προγραμμάτων και εγγράφων). Τα αρχεία λαμβάνονται τοπικά όπως και στην πρώτη περίπτωση αλλά δεν διασφαλίζεται η σωστή κοινή χρήση τους. Για αυτό τον λόγο συνιστάται για φακέλους που περιέχουν αρχεία μόνο για ανάγνωση ή εφαρμογές οι οποίες εκτελούνται δικτυακά.
- iii. **Manual Caching for Documents** (Μη αυτόματη προσωρινή αποθήκευση εγγράφων). Οι χρήστες πρέπει να καθορίσουν οι ίδιοι τα αρχεία που θέλουν να είναι διαθέσιμα offline, κάνοντας δεξί κλικ στο αρχείο που τους ενδιαφέρει και επιλέγοντας Make Available Offline (Διαθέσιμο για εργασία χωρίς σύνδεση). Για να διασφαλιστεί η σωστή κοινή χρήση των αρχείων ανοίγεται πάντα η έκδοση του διακομιστή του αρχείου. Συνιστάται για φακέλους οι οποίοι περιέχουν έγγραφα χρήστη.

Όταν μοιράζουμε έναν φάκελο από προεπιλογή είναι διαθέσιμος offline με Manual Caching for Documents (Μη αυτόματη προσωρινή αποθήκευση εγγράφων).



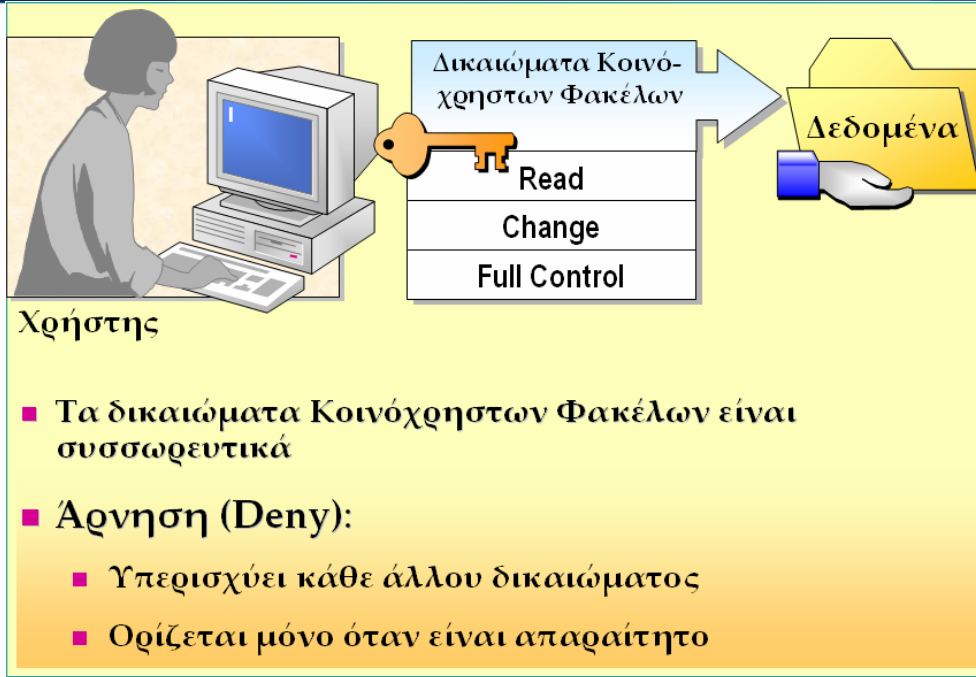
## Δικαιώματα Κοινόχρηστων Φακέλων

Ορίζοντας τα δικαιώματα των χρηστών για έναν κοινόχρηστο φάκελο μπορούμε είτε να εκχωρήσουμε ένα δικαίωμα είτε να το αρνηθούμε. Τα δικαιώματα αυτά εφαρμόζονται μόνο όταν ο χρήστης συνδέεται με τον φάκελο μέσω του δικτύου· δεν περιορίζουν την πρόσβαση όταν ο χρήστης “κάθεται τοπικά” στον υπολογιστή στον οποίο βρίσκεται ο φάκελος. Μπορούμε να ορίσουμε δικαιώματα Κοινόχρηστου Φακέλου για Λογαριασμό Χρήστη ή Ομάδα Χρηστών.

Για να ελέγξουμε την πρόσβαση των χρηστών στους κοινόχρηστους φακέλους χρησιμοποιούμε τα δικαιώματα. Τα δικαιώματα αυτά μπορούν να οριστούν μόνο στον κοινόχρηστο φάκελο συνολικά και όχι σε μεμονωμένα αρχεία που περιέχονται στον φάκελο.

Ο παρακάτω πίνακας περιγράφει τι επιτρέπεται στον χρήστη ανάλογα με τα δικαιώματα που του έχουν εκχωρηθεί:

<b>Read</b>	Εμφάνιση ονομάτων φακέλων, ονομάτων αρχείων, δεδομένων αρχείων και ιδιοτήτων· εκτέλεση αρχείων εφαρμογών.
<b>Change</b>	Δημιουργία υποφακέλων· προσθήκη αρχείων στους φακέλους· αλλαγή δεδομένων αρχείων· προσθήκη δεδομένων στα αρχεία· αλλαγή ιδιοτήτων αρχείων· διαγραφή αρχείων και φακέλων.
<b>Full Control</b>	Αλλαγή δικαιωμάτων ασφάλειας NTFS αρχείων και φακέλων· απόκτηση ιδιοκτησίας (Take Ownership) αρχείων και φακέλων και όλα τα άλλα δικαιώματα Change και Read. Από προεπιλογή η ομάδα Everyone έχει Full Control.



### Τα δικαιώματα είναι συσσωρευτικά.

Τα δικαιώματα τα οποία τελικά ένας χρήστης έχει σε έναν κοινόχρηστο φάκελο είναι ο συνδυασμός των δικαιωμάτων που του έχουν εκχωρηθεί στον κοινόχρηστο φάκελο ως μεμονωμένου χρήστη και των δικαιωμάτων που έχουν εκχωρηθεί στις ομάδες χρηστών στις οποίες ανήκει. Για παράδειγμα αν ένας χρήστης έχει Read δικαίωμα σε έναν κοινόχρηστο φάκελο, αλλά είναι και μέλος μίας ομάδας η οποία έχει δικαίωμα Change στον ίδιο φάκελο, τότε ο χρήστης έχει δικαιώματα Read και Change σε αυτόν τον φάκελο.

### Η Άρνηση (Deny) υπερισχύει κάθε άλλου εκχωρημένου δικαιώματος.

Συνιστάται να χρησιμοποιείτε την Άρνηση (Deny) δικαιωμάτων σε έναν κοινόχρηστο φάκελο ΜΟΝΟ όταν θέλετε να διασφαλίσετε ότι ένας συγκεκριμένος χρήστης δεν θα έχει πρόσβαση σε έναν κοινόχρηστο φάκελο, ακόμη και όταν εκχωρήσετε δικαιώματα στην ομάδα στην οποία ανήκει αυτός ο χρήστης. Αν απλώς δεν εκχωρήσετε κανένα δικαίωμα στον συγκεκριμένο χρήστη αυτός μπορεί να αποκτήσει πρόσβαση αν μια από τις ομάδες χρηστών στις οποίες ανήκει έχει δικαίωμα πρόσβασης.

**Σημαντικό** Αν θέλετε να εκχωρήσετε δικαιώματα μόνο σε ορισμένους χρήστες καταργήστε (Remove) την ομάδα Everyone, αλλιώς όλοι οι χρήστες θα έχουν δικαιώματα Full Control στον κοινόχρηστο φάκελο. Αν αλλάξετε το δικαίωμα της ομάδας Everyone σε Άρνηση (Deny) κανείς απολύτως χρήστης δεν θα έχει δικαίωμα πρόσβασης στον κοινόχρηστο



φάκελο, συμπεριλαμβανομένων των χρηστών που θέλετε να έχουν πρόσβαση.



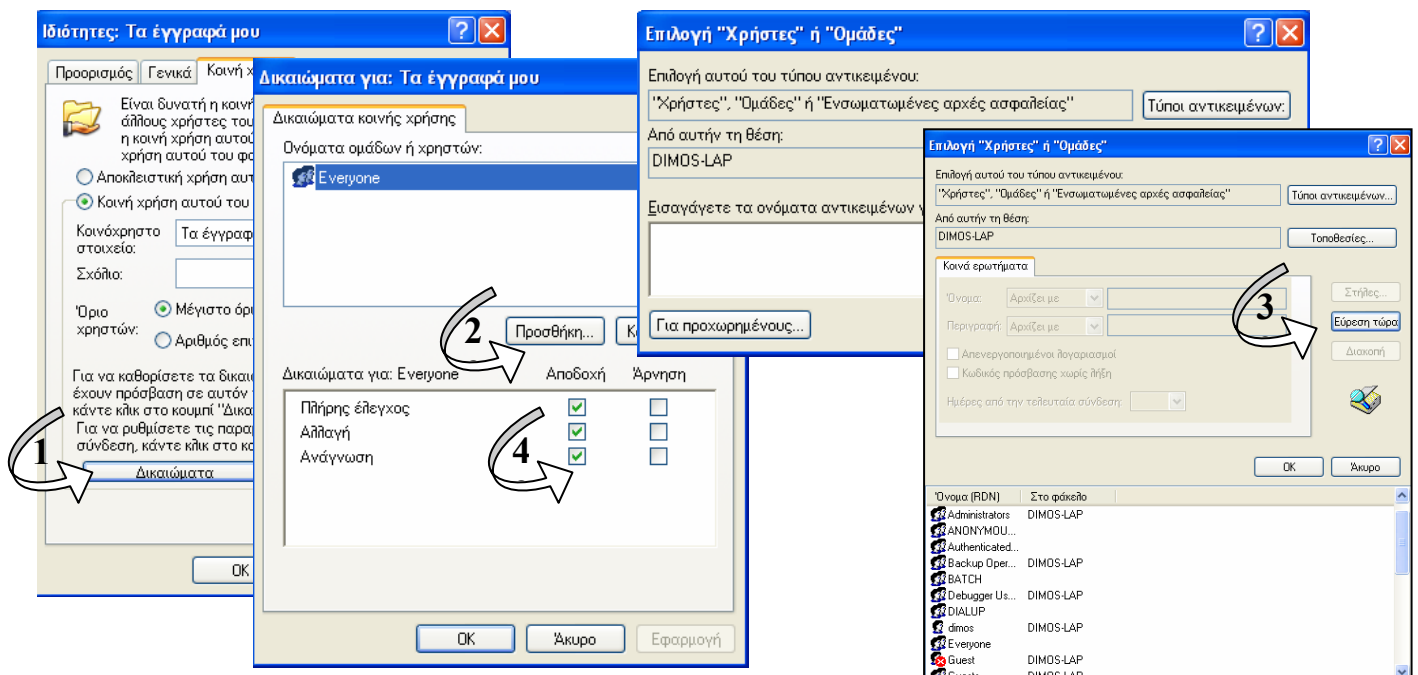
## Εκχώρηση δικαιωμάτων Κοινόχρηστου Φακέλου

Αφού “μοιράσουμε” έναν φάκελο μπορούμε να ελέγξουμε ποιους λογαριασμοί χρηστών ή ομάδες χρηστών έχουν πρόσβαση μέσω των δικαιωμάτων κοινόχρηστων φακέλων.

**Σημαντικό** για να έχει πρόσβαση κάποιος χρήστης σε ένα κοινόχρηστο φάκελο πρέπει να έχει τα κατάλληλα NTFS δικαιώματα για κάθε αρχείο και φάκελο, επιπρόσθετα από τα δικαιώματα κοινόχρηστου φακέλου. Τα NTFS δικαιώματα ορίζονται από την καρτέλα Ασφάλεια (Security) του πλαισίου διαλόγου “Ιδιότητες” του φακέλου.

Για την εκχώρηση δικαιωμάτων κοινόχρηστων φακέλων σε χρήστες ή ομάδες, κάνουμε τα ακόλουθα βήματα:

1. ανοίγουμε το πλαίσιο διαλόγου Ιδιότητες του κοινόχρηστου φακέλου, και στην καρτέλα Κοινή Χρήση (Sharing) κάνουμε κλικ στο Δικαιώματα για να ανοίξει το αντίστοιχο πλαίσιο διαλόγου.
2. Επιλέγουμε “Προσθήκη...” (Add...). Στο πλαίσιο διαλόγου “Επιλογή χρήστες ή ομάδες” κάνουμε κλικ στο “Τοποθεσίες...” για να δούμε μία λίστα με τους τομείς (Domains), συμπεριλαμβανομένου και του τοπικού υπολογιστή, ή επιλέγουμε “για προχωρημένους” και “Εύρεση τώρα” όπου μπορούμε να επιλέξουμε λογαριασμούς χρηστών και ομάδες.
3. Επιλέγουμε τον λογαριασμό χρήστη ή την ομάδα στην οποία θέλουμε να εκχωρήσουμε δικαιώματα.
4. Τσεκάρουμε το πλαίσιο “Αποδοχή” στο δικαίωμα που θέλουμε να εκχωρήσουμε στον χρήστη ή στην ομάδα.







## Τροποποίηση ρυθμίσεων Κοινόχρηστου Φακέλου

Μπορούμε να τροποποιήσουμε τους κοινόχρηστους φακέλους από την καρτέλα “κοινή χρήση” του πλαισίου διαλόγου Ιδιότητες.

- Για να σταματήσουμε την κοινή χρήση ενός φακέλου επιλέγουμε “Αποκλειστική χρήση αυτού του φακέλου”.
- Για να αλλάξουμε το όνομα με το οποίο “μοιράζεται” ένας φάκελος πρέπει πρώτα να διακόψουμε “μοίρασμά” του επιλέγοντας “Αποκλειστική χρήση αυτού του φακέλου” → “Εφαρμογή” κατόπιν επιλέγουμε “Κοινή χρήση αυτού του φακέλου” και γράφουμε το νέο όνομα στο πλαίσιο “κοινόχρηστο στοιχείο”.
- Τα δικαιώματα τροποποιούνται με την ίδια διαδικασία που ορίζονται.
- Μπορούμε να “μοιράσουμε ” έναν κοινόχρηστο φάκελο πολλές φορές με διαφορετικά ονόματα και δικαιώματα, επιλέγοντας “Νέο κοινόχρηστο στοιχείο”. Χρησιμοποιούμε τα πρόσθετα ονόματα όταν θέλουμε να συγχωνεύσουμε πολλούς κοινόχρηστους φακέλους σε έναν. Έτσι οι χρήστες συνεχίζουν να χρησιμοποιούν το αρχικό κοινόχρηστο όνομα του φακέλου. Αυτή η επιλογή εμφανίζεται μόνο όταν ο φάκελος είναι ήδη κοινόχρηστος.
- Με την επιλογή “κατάργηση κοινής χρήσης” μπορούμε να καταργήσουμε ένα από τα κοινόχρηστα ονόματα του φακέλου. Η επιλογή αυτή εμφανίζεται όταν έχουμε “μοιράσει” έναν φάκελο πάνω από μία φορά.

**Σημαντικό** Αν διακόψουμε το μοίρασμα ενός φακέλου την ώρα που κάποιος δουλεύει με ένα αρχείου του φακέλου, είναι πιθανό ο χρήστης να χάσει δεδομένα. Γι’ αυτό το λόγο, στα Windows 2000, εμφανίζεται ένα πλαίσιο διαλόγου που μας ενημερώνει ότι κάποιος χρήστης είναι συνδεδεμένος.

Αν αλλάξουμε το κοινόχρηστο όνομα ενός φακέλου, αφαιρούνται όλα τα δικαιώματα που έχουμε εκχωρήσει και θα πρέπει να τα ξαναορίσουμε.

Αν μεταφέρουμε έναν κοινόχρηστο φάκελο παύει να είναι κοινόχρηστος. Το ίδιο συμβαίνει και αν μετονομάσουμε έναν φάκελο που “μοιράζεται”.





## Κοινόχρηστοι Φάκελοι Διαχείρισης

Τα Windows 2000 αυτόματα μοιράζουν φακέλους που μας επιτρέπουν να εκτελέσουμε διαχειριστικές εργασίες. Στο κοινόχρηστο όνομα αυτών των φακέλων προστίθεται το σύμβολο του δολαρίου (\$). Το \$ κρύβει τον κοινόχρηστο φάκελο από τους χρήστες όταν αυτοί αναζητούν υπολογιστές στην Περιοχή Δικτύου.

Από προεπιλογή η ομάδα των Administrators έχει δικαιώματα Full Control σε αυτούς τους φακέλους. Δεν μπορούμε να τροποποιήσουμε τα δικαιώματα των Κοινόχρηστων Φακέλων Διαχείρισης (εκτός του Print\$). Ο παρακάτω πίνακας περιγράφει τον σκοπό των κοινόχρηστων φακέλων διαχείρισης που παρέχουν αυτόματα τα Windows 2000:

Κοινόχρηστος Φάκελος	Σκοπός
C\$, D\$, E\$, κ.ο.κ.	Χρησιμοποιούνται κατά την απομακρυσμένη σύνδεση με έναν υπολογιστή για την διενέργεια εργασιών διαχείρισης. Το root του κάθε διαμερίσματος των σκληρών δίσκων, καθώς και των CD-ROM, μοιράζεται αυτόματα. Όταν συνδεόμαστε σε αυτό έχουμε πρόσβαση σε ολόκληρο το διαμέρισμα (Partition)
Admin\$	Ο φάκελος εγκατάστασης του συστήματος (system root), που συνήθως είναι ο C:\Winnt. Ο διαχειριστής μπορεί να συνδεθεί στον φάκελο αυτό για να διαχειριστεί τα Windows 2000 χωρίς να ξέρει ποιος είναι ο φάκελος εγκατάστασης.
Print\$	Δίνει πρόσβαση στους οδηγούς εγκατάστασης εκτυπωτών για τους υπολογιστές-πελάτες. Όταν εγκαταστήσουμε πρώτη φορά και μοιράσουμε έναν εκτυπωτή, ο φάκελος <i>systemroot/System32/Spool/Drivers</i> γίνεται κοινόχρηστος με το όνομα Print\$. Μόνο μέλη των ομάδων Administrators, Server Operators και Print Operators έχουν Full Control. Η ομάδα Everyone έχει Read.

Οι κρυφοί κοινόχρηστοι φάκελοι δεν περιορίζονται μόνο στους κοινόχρηστους φακέλους διαχείρισης που δημιουργούν τα Windows 2000. Μπορούμε να μοιράσουμε και άλλους φακέλους, που με την προσθήκη του \$ στο κοινόχρηστο όνομά τους γίνονται κρυφοί, ώστε μόνο οι χρήστες που ξέρουν το όνομά τους να μπορούν να τους εντοπίσουν.



## Ασφάλεια

### Δικαιώματα NTFS

Τα δικαιώματα NTFS μπορούν να οριστούν μόνο σε δίσκους ή διαμερίσματα δίσκων που είναι διαμορφωμένα με το σύστημα NTFS (New Technology File System).

Χρησιμοποιούμε τα δικαιώματα NTFS για να ορίσουμε ποιοι χρήστες ή ομάδες χρηστών έχουν πρόσβαση σε αρχεία και φακέλους. Επίσης τα δικαιώματα NTFS καθορίζουν τι μπορούν να κάνουν οι χρήστες ή οι ομάδες με τα περιεχόμενα των αρχείων ή φακέλων.

### Δικαιώματα NTFS φακέλων

<b>Read</b>	Προβολή αρχείων, φακέλων και υποφακέλων, καθώς και προβολή των ιδιοτήτων, ιδιοκτησίας και δικαιωμάτων.
<b>Write</b>	Δημιουργία νέων αρχείων και υποφακέλων μέσα στον φάκελο, αλλαγή χαρακτηριστικών (attributes) και ότι το Read
<b>List Folder Contents</b>	Προβολή ονομάτων αρχείων και υποφακέλων του φακέλου
<b>Read &amp; Execute</b>	Μετακίνηση μέσα σε υποφακέλους για τον εντοπισμό άλλων αρχείων ή φακέλων έστω και αν ο χρήστης δεν έχει δικαιώματα για τους διατρεχόμενους φακέλους, και ότι ισχύει για τα δικαιώματα Read και List Folder Contents
<b>Modify</b>	Διαγραφή φακέλων και ότι ισχύει για τα δικαιώματα Write και Read & Execute
<b>Full control</b>	Αλλαγή δικαιωμάτων NTFS απόκτηση ιδιοκτησίας (Take Ownership) αρχείων και φακέλων, διαγραφή αρχείων και φακέλων, και ότι επιτρέπεται από τα άλλα δικαιώματα NTFS.



### Δικαιώματα NTFS αρχείων

<b>Read</b>	Ανάγνωση αρχείου και προβολή χαρακτηριστικών, ιδιοκτησίας και δικαιωμάτων του.
<b>Write</b>	Αλλαγή αρχείου (overwrite), αλλαγή χαρακτηριστικών του (Attributes) και προβολή ιδιοκτησίας και δικαιωμάτων.
<b>Read &amp; Execute</b>	Εκτέλεση εφαρμογών και ότι επιτρέπεται από το Read.
<b>Modify</b>	Τροποποίηση και διαγραφή αρχείου και ότι επιτρέπεται από το Write και Read & Execute.
<b>Full control</b>	Αλλαγή δικαιωμάτων, απόκτηση ιδιοκτησίας (Take Ownership) αρχείου και ότι επιτρέπεται από τα άλλα δικαιώματα NTFS

**Σημαντικό** Όταν διαμορφώνουμε ένα διαμέρισμα δίσκου σε NTFS, τα Windows 2000 αυτόματα δίνουν δικαίωμα Full Control στο Root στην ομάδα Everyone. Από προεπιλογή η ομάδα Everyone θα έχει Full Control σε όλα τα αρχεία και φακέλους που δημιουργούνται. Για να περιορίσουμε την πρόσβαση μόνο στους χρήστες που επιθυμούμε θα πρέπει να αλλάξουμε τα προεπιλεγμένα δικαιώματα στα αρχεία και φακέλους που δημιουργούμε.

### Πολλαπλά Δικαιώματα NTFS

Αν εκχωρήσουμε δικαιώματα NTFS σε έναν χρήστη και στην ομάδα ή ομάδες στις οποίες ανήκει τότε του έχουμε δώσει πολλαπλά δικαιώματα NTFS. Υπάρχουν κανόνες για το πώς το NTFS συνδυάζει αυτά τα δικαιώματα για να εξαγάγει τα δικαιώματα που θα ισχύσουν.

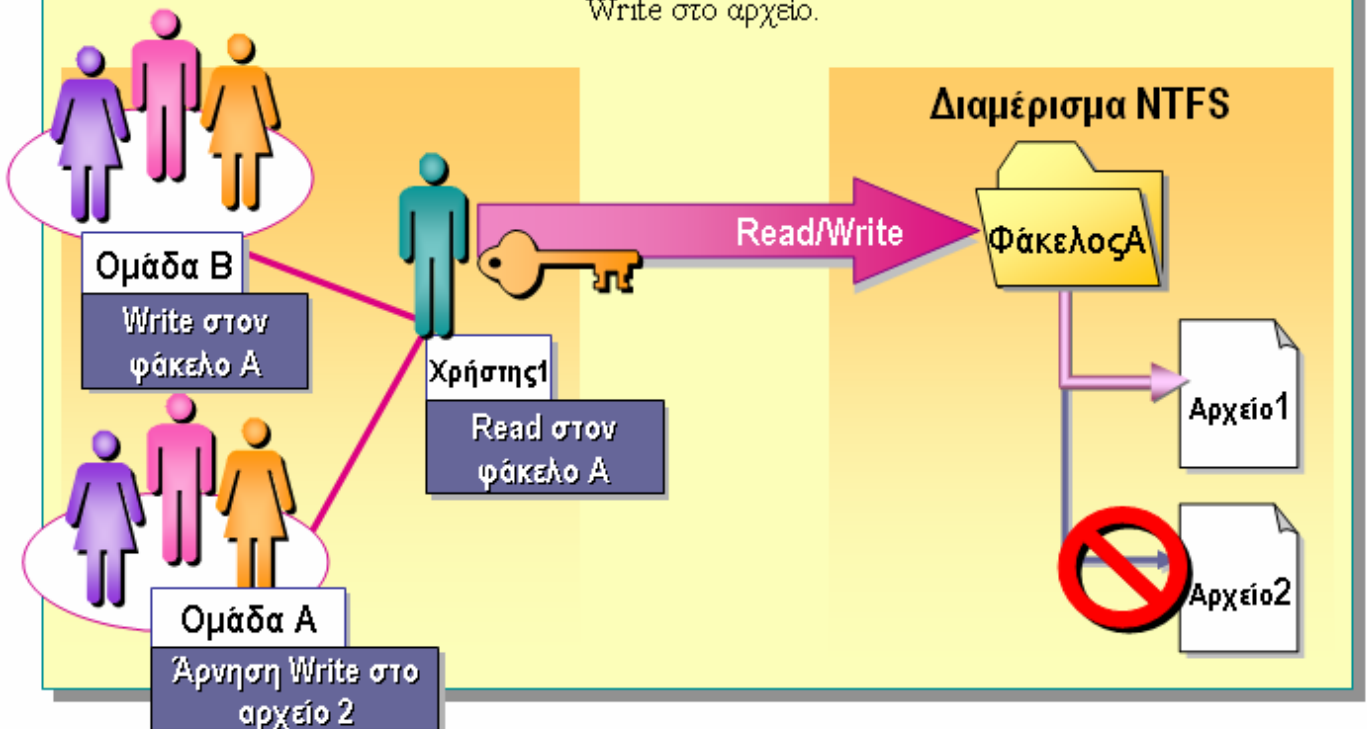
- **Τα δικαιώματα είναι συσσωρευτικά.** Τα δικαιώματα που θα ισχύουν για έναν χρήστη είναι ο συνδυασμός των NTFS δικαιωμάτων που έχει ο χρήστης ατομικά και των δικαιωμάτων που έχει μέσω της συμμετοχής του σε ομάδες. Για παράδειγμα αν ένας χρήστης έχει δικαίωμα Read σε έναν φάκελο και ανήκει σε μία ομάδα που έχει Write στον ίδιο φάκελο, ο χρήστης τελικά θα έχει Read και Write.
- **Τα δικαιώματα αρχείων είναι ξεχωριστά από τα δικαιώματα φακέλων.** Τα δικαιώματα NTFS αρχείων έχουν προτεραιότητα



έναντι των δικαιωμάτων NTFS φακέλων. Για παράδειγμα ένας χρήστης με δικαίωμα Modify σε ένα αρχείο θα μπορεί να κάνει αλλαγές σε αυτό ακόμη και αν έχει μόνο Read δικαίωμα στον φάκελο που περιέχει το αρχείο.

- Η **Άρνηση (Deny)** υπερισχύει κάθε άλλου εκχωρημένου δικαιώματος. Μπορούμε να απαγορεύσουμε την πρόσβαση σε ένα αρχείο ή φάκελο χρησιμοποιώντας την Άρνηση (Deny) σε έναν χρήστη ή ομάδα. Ακόμη και αν ο χρήστης έχει δικαίωμα πρόσβασης μέσω μίας ομάδας στην οποία ανήκει, η Άρνηση μπλοκάρει οποιαδήποτε δικαιώματα μπορεί να έχει. Γι' αυτό η **Άρνηση αποτελεί εξαίρεση στον κανόνα συσσώρευσης των δικαιωμάτων.**

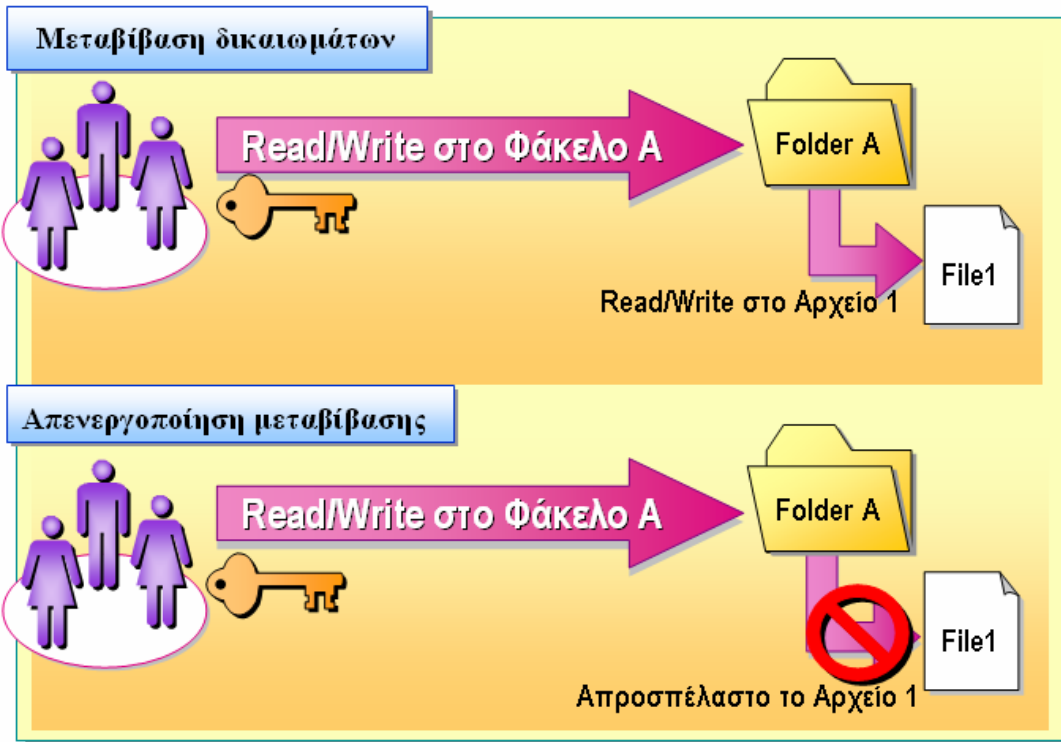
Ο Χρήστης1 ανήκει σε δύο ομάδες την A και B. Αν και στον ίδιο έχει εκχωρηθεί μόνο Read στον φάκελο A, η πρόσβαση που έχει στον φάκελο είναι Read και Write επειδή είναι μέλος της ομάδας B που έχει Write. Έτσι μπορεί να αλλάξει το αρχείο 1 αφού η πρόσβαση του είναι Read/Write. Παράλληλα όμως αν και έχει πρόσβαση Read/Write στο φάκελο A, δεν του επιτρέπεται η πρόσβαση στο αρχείο 2 επειδή είναι μέλος της ομάδας A που έχει Άρνηση (Deny) Write στο αρχείο.





## Μεταβίβαση δικαιωμάτων NTFS

Από προεπιλογή, τα δικαιώματα NTFS που ορίζονται σε έναν φάκελο μεταβιβάζονται και αναπαράγονται στους υποφακέλους και τα αρχεία που περιέχονται στον πατρικό φάκελο. Ωστόσο μπορούμε να εμποδίσουμε την μεταβίβαση αυτή αν θέλουμε οι φάκελοι και τα αρχεία να έχουν διαφορετικά δικαιώματα από τον πατρικό φάκελο.



### Μεταβίβαση δικαιωμάτων

Όποια δικαιώματα και αν δώσουμε στον πατρικό φάκελο, εφαρμόζονται και στα αρχεία και υποφακέλους που περιέχει. Εκχωρώντας δικαιώματα NTFS για να ελέγξουμε την πρόσβαση σε έναν φάκελο, εκχωρούμε τα δικαιώματα αυτά στον φάκελο, σε όλα τα υπάρχοντα αρχεία και φακέλους, καθώς και σε όποια αρχεία ή φακέλους θα δημιουργήσουμε μέσα στον φάκελο στο μέλλον.

### Απενεργοποίηση μεταβίβασης δικαιωμάτων

Μπορούμε να εμποδίσουμε την μεταβίβαση δικαιωμάτων και έτσι να διατηρήσουμε μόνο τα δικαιώματα που έχουν εκχωρηθεί ρητώς (explicitly) σε έναν φάκελο ή αρχείο. Όταν απενεργοποιούμε την μεταβίβαση των δικαιωμάτων μπορούμε να επιλέξουμε να αντιγράψουμε τα ήδη μεταβιβασθέντα δικαιώματα.

Ο υποφάκελος στον οποίο απενεργοποιούμε την μεταβίβαση δικαιωμάτων από τον πατρικό του φάκελο γίνεται ένας νέος πατρικός



φάκελος, ο οποίος θα μεταβιβάζει και αναπαράγει τα δικαιώματα που του εκχωρούμε στα αρχεία και τους υποφακέλους που περιέχει.

### **Αντιγραφή και Μετακίνηση Αρχείων και Φακέλων**

Για να αντιγράψουμε ένα αρχείο ή φάκελο πρέπει να έχουμε τουλάχιστον δικαιώματα Read στο στοιχείο (αρχείο ή φάκελος) προέλευσης και Write στον φάκελο προορισμού.

Για να μετακινήσουμε ένα αρχείο ή φάκελο πρέπει να έχουμε δικαιώματα Modify στο στοιχείο προέλευσης και Write στον φάκελο προορισμού.

Η μετακίνηση ή αντιγραφή αρχείων και φακέλων επηρεάζει τα δικαιώματα NTFS.

Κατά την αντιγραφή το αρχείο ή ο φάκελος κληρονομεί δικαιώματα από τον φάκελο προορισμού ανεξάρτητα από το αν ο φάκελος προορισμού βρίσκεται στο ίδιο ή σε διαφορετικό διαμέρισμα NTFS .

Κατά την μετακίνηση ενός φακέλου:

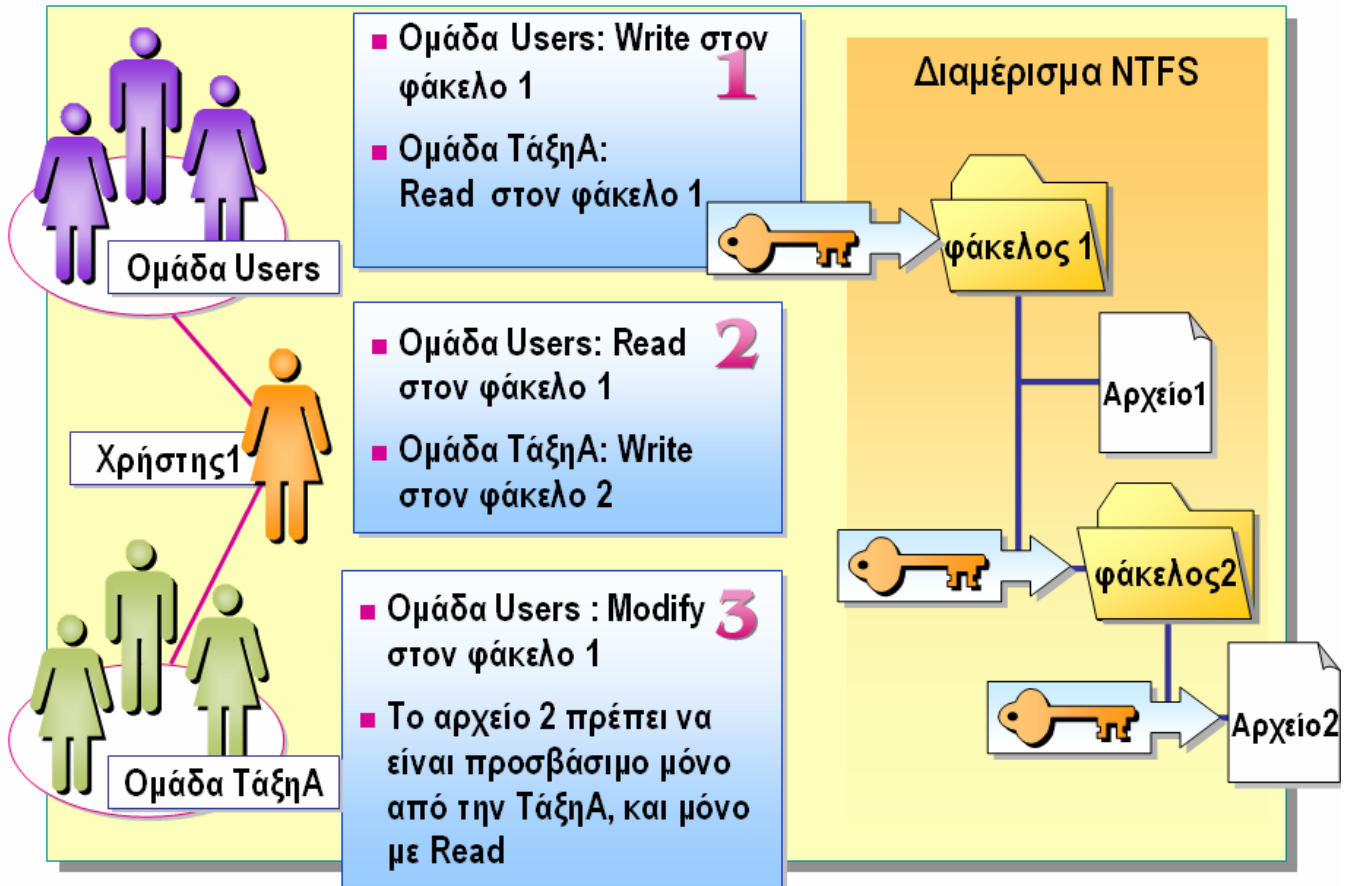
- Αν μετακινήσουμε ένα φάκελο ή αρχείο μέσα στο ίδιο διαμέρισμα NTFS, ο φάκελος ή το αρχείο διατηρεί τα αρχικά του δικαιώματα.
- Αν μετακινήσουμε ένα φάκελο ή αρχείο σε διαφορετικό διαμέρισμα NTFS, ο φάκελος ή το αρχείο κληρονομεί τα δικαιώματά του από τον φάκελο προορισμού.

Φυσικά η μετακίνηση ή αντιγραφή σε διαμέρισμα που δεν είναι NTFS (FAT, FAT32), δεν περιλαμβάνει τα δικαιώματα του αρχείου ή του φακέλου.





## Εφαρμογή δικαιωμάτων NTFS



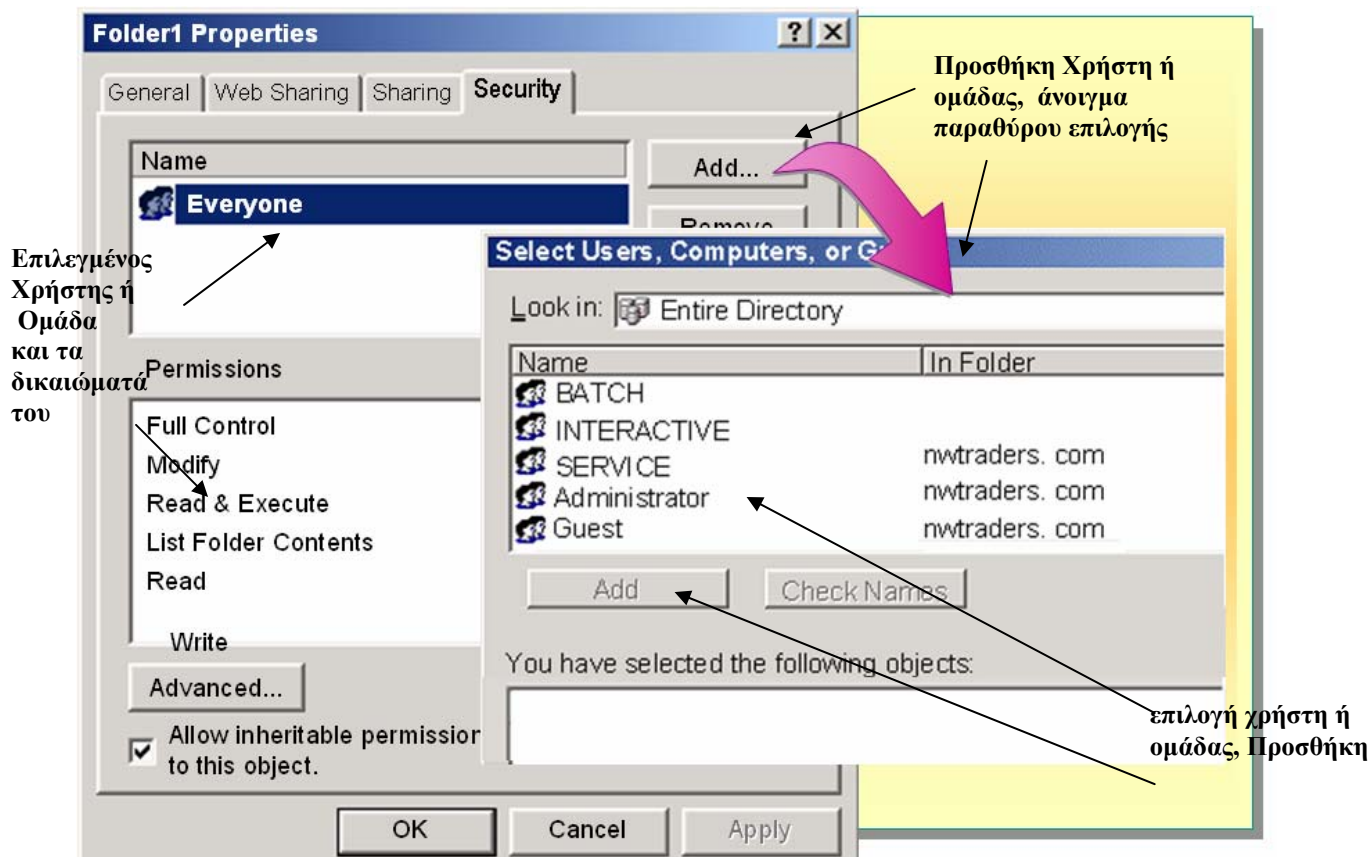
Ο χρήστης 1 είναι μέλος των ομάδων Users και ΤάξηΑ.

1. Η ομάδα Users έχει δικαίωμα Write και η ομάδα ΤάξηΑ Read στον φάκελο 1. Τι δικαιώματα έχει ο Χρήστης1 στον φάκελο 1;
2. Η ομάδα Users έχει δικαίωμα Read. η ομάδα ΤάξηΑ έχει δικαίωμα Write στον φάκελο 2. Τι δικαιώματα έχει ο Χρήστης1 στον φάκελο 2;
3. Η ομάδα Users έχει δικαίωμα Modify στον φάκελο 1. Μόνο οι χρήστες που ανήκουν στην ομάδα ΤάξηΑ πρέπει να έχουν πρόσβαση στο αρχείο 2, και μόνο με δικαίωμα Read. Πώς θα εξασφαλίσουμε ότι μόνο η ΤάξηΑ έχει δικαίωμα Read στο αρχείο 2;



## Εκχώρηση δικαιωμάτων NTFS

Εκχωρούμε δικαιώματα NTFS από το πλαίσιο διαλόγου “Ιδιότητες (Properties)” του αρχείου ή φακέλου, και την καρτέλα “Ασφάλεια (Security)”.



Όταν εκχωρούμε ή τροποποιούμε δικαιώματα NTFS σε έναν χρήστη ή ομάδα, μπορούμε να προσθέσουμε ή να αφαιρέσουμε χρήστες ή ομάδες από το αρχείο ή τον φάκελο. Επιλέγοντας έναν χρήστη ή ομάδα μπορούμε να τροποποιήσουμε τα δικαιώματά του.





Στην καρτέλα “Ασφάλεια” ρυθμίζουμε τις εξής επιλογές:

Επιλογή	Περιγραφή
Name Ονόματα ομάδων ή Χρηστών	Επιλέγουμε τον χρήστη ή την ομάδα του οποίου τα δικαιώματα θέλουμε να αλλάξουμε ή να τα καταργήσουμε.
Permissions Δικαιώματα	Εκχωρείται το δικαίωμα που έχουμε τσεκάρει στην στήλη “Αποδοχή” (Allow) Αφαιρείται το δικαίωμα που έχουμε τσεκάρει στην στήλη “Άρνηση” (Deny)
Add Προσθήκη	Ανοίγει το πλαίσιο διαλόγου “Προσθήκη χρηστών και ομάδων” που το χρησιμοποιούμε για να επιλέξουμε τους χρήστες και τις ομάδες που θέλουμε να προσθέσουμε στο πεδίο “Ονόματα ομάδων ή Χρηστών”
Remove Κατάργηση	Απομακρύνει τον επιλεγμένο χρήστη ή ομάδα και καταργεί όλα τα δικαιώματα που σχετίζονταν με αυτόν και το αρχείο ή τον φάκελο.

Από προεπιλογή τα Windows 2000 εκχωρούν το δικαίωμα Full Control στην ομάδα Everyone όταν δημιουργείται ένας φάκελος ή ένα αρχείο, ή όταν διαμορφώνεται ένα διαμέρισμα σε NTFS.



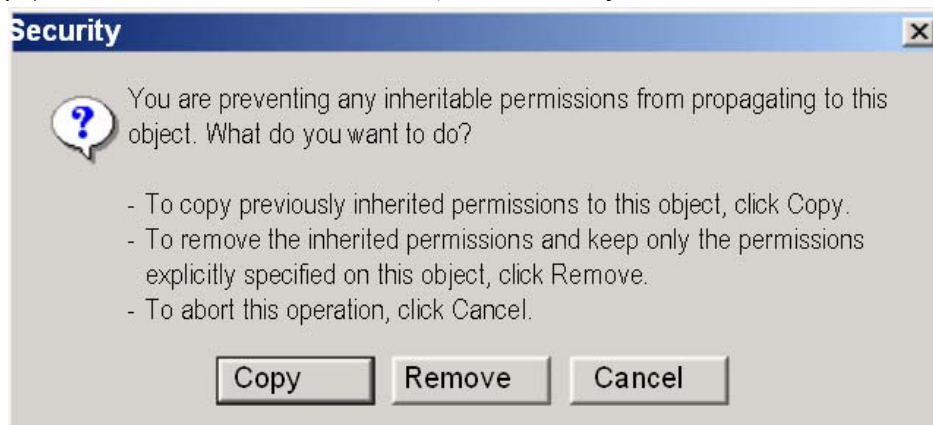
## Ρύθμιση Μεταβίβασης Δικαιωμάτων

Γενικά αφήνουμε τα Windows 2000 να αναπαράγουν τα δικαιώματα NTFS του πατρικού φακέλου σε όλα τα αρχεία και υποφακέλους που περιέχει, απλοποιώντας έτσι την εκχώρηση δικαιωμάτων των πόρων.

Ωστόσο, μερικές φορές, μπορεί να θελήσουμε να εμποδίσουμε την μεταβίβαση αυτή. Για παράδειγμα έχουμε ένα φάκελο "Εργασίες" στον οποίο οι χρήστες της ομάδας "ΤάξηΑ" πρέπει να έχουν πρόσβαση Write ώστε να μπορούν να δημιουργούν ή να αντιγράφουν στο φάκελο τις εργασίες τους. Στον ίδιο φάκελο θα βρουν και το αρχείο "Οδηγίες για την Εργασία σας" το οποίο βέβαια δεν θα πρέπει να μπορούν να τροποποιήσουν. Για να το πετύχουμε αυτό θα διακόψουμε την μεταβίβαση των δικαιωμάτων σε αυτό το αρχείο ώστε να μην αναπαραχθεί το δικαίωμα Write από τον πατρικό φάκελο "Εργασίες".

Πως το κάνουμε:

- Ανοίγουμε το παράθυρο ιδιοτήτων του αρχείου "Οδηγίες για την Εργασία σας" ( δεξί κλικ στο αρχείο → "Ιδιότητες" (Properties).
- Στην καρτέλα "Ασφάλεια" (Security), αποεπιλέγουμε το πλαίσιο "Μεταβίβαση των καταχωρήσεων δικαιωμάτων" (Allow inheritable permissions from parent to propagate).
- Εμφανίζεται το πλαίσιο διαλόγου "Security"









και επιλέγουμε:

- Copy αν θέλουμε να αντιγραφούν τα δικαιώματα που έχουν ήδη μεταβιβαστεί και να σταματήσει από εδώ και στο εξής η μεταβίβαση
- Remove αν θέλουμε να καταργηθούν όλα τα δικαιώματα που έχουν μεταβιβαστεί από τον πατρικό φάκελο. Θα διατηρηθούν μόνο τα δικαιώματα που έχουν ρητώς εκχωρηθεί στο συγκεκριμένο αρχείο ή φάκελο.



## Συνιστώμενες Πρακτικές

Λάβετε υπ' όψιν σας τις ακόλουθες πρακτικές σχετικά με την εκχώρηση δικαιωμάτων NTFS :

-  **Εκχώρηση δικαιωμάτων σε Ομάδες παρά σε Χρήστες**
-  **Ομαδοποίηση των πόρων για απλοποίηση της διαχείρισης**
-  **Εκχωρήστε το ελάχιστο επίπεδο πρόσβασης που χρειάζεται**
-  **Δημιουργήστε ομάδες ανάλογα με την πρόσβαση που χρειάζονται**
-  **Εκχωρήστε δικαίωμα Read & Execute σε φακέλους εφαρμογών**
-  **Εκχωρήστε δικαίωμα Write/Read & Execute σε φακέλους δεδομένων**

- Εκχωρείτε δικαιώματα σε ομάδες παρά σε χρήστες. Είναι ευκολότερο να διαχειριζόμαστε ομάδες από χρήστες. Επίσης με αυτήν την πρακτική αυξάνει η απόδοση του συστήματος.
- Για την απλοποίηση της διαχείρισης συγκεντρώστε τα αρχεία εφαρμογών εκεί που είναι και οι εφαρμογές τους, τα κοινόχρηστα αρχεία που χρησιμοποιούνται από πολλούς χρήστες, τα προσωπικά αρχεία δεδομένων με τους Home Folders των χρηστών. Συγκεντρώστε τους Home Folders και τους φακέλους δεδομένων των χρηστών σε διαφορετικό διαμέρισμα.
- Εκχωρήστε τα ελάχιστα δικαιώματα που χρειάζεται ένας χρήστης ή ομάδα. Αν ένας χρήστης χρειάζεται να διαβάζει ένα αρχείο, εκχωρήστε του μόνο το δικαίωμα Read.
- Δημιουργήστε ομάδες με βάση το είδος πρόσβασης που χρειάζονται τα μέλη τους, και μετά εκχωρήστε τα ανάλογα δικαιώματα στις ομάδες.
- Όταν εκχωρείτε δικαιώματα σε φακέλους με εφαρμογές, εκχωρήστε Read & Execute στις ομάδες Users και Administrators. Με αυτόν τον τρόπο προλαμβάνεται την διαγραφή δεδομένων και αρχείων εφαρμογών από λάθος χρήστη ή από ιούς.
- Στους φακέλους δεδομένων δώστε Read & Execute και Write στην ομάδα Users και Full Control στον λογαριασμό Owner. Με αυτό τον τρόπο οι χρήστες έχουν την δυνατότητα να διαβάζουν και να τροποποιούν αρχεία άλλων χρηστών αλλά να διαγράφουν μόνο τα αρχεία και φακέλους που έφτιαξαν οι ίδιοι.



## Συνδυασμός δικαιωμάτων NTFS και Κοινής Χρήσης

Όταν μοιράζουμε έναν φάκελο που βρίσκεται σε διαμέρισμα διαμορφωμένο ως NTFS, τα δικαιώματα κοινής χρήσης συνδυάζονται με τα δικαιώματα ασφάλειας NTFS.

Οι χρήστες πρέπει να έχουν τα κατάλληλα δικαιώματα NTFS για κάθε αρχείο και υποφάκελο του κοινόχρηστου φακέλου, επιπρόσθετα από τα δικαιώματα κοινής χρήσης που του έχετε εκχωρήσει για να έχει πρόσβαση στους πόρους του κοινόχρηστου φακέλου.

Όταν συνδυάζονται τα δικαιώματα NTFS με τα δικαιώματα κοινόχρηστου φακέλου το αποτέλεσμα είναι να ισχύσουν τα πιο ΠΕΡΙΟΡΙΣΤΙΚΑ για τον χρήστη δικαιώματα είτε αυτά είναι NTFS είτε Κοινής Χρήσης.

### Παράδειγμα

Ο χρήστης Γεωργίου είναι μέλος των ομάδων Users και ΤάξηΓ. Ο φάκελος A, που βρίσκεται σε NTFS διαμέρισμα, μοιράζεται και έχουν εκχωρηθεί τα εξής δικαιώματα:

Γεωργίου: Full Control

Users: Read

ΤάξηΓ: Modify

Παράλληλα έχουν οριστεί τα εξής δικαιώματα NTFS :

Users: Read

Γεωργίου: Write

Τι είδους πρόσβαση έχει τελικά ο χρήστης Γεωργίου στον φάκελο A;

- Αν προσεγγίσει τον φάκελο τοπικά θα εφαρμοστούν μόνο τα δικαιώματα NTFS, που επειδή είναι πολλαπλά θα δράσουν συσσωρευτικά δηλαδή θα έχει δικαιώματα Read και Write.
- Αν προσεγγίσει το φάκελο μέσω δικτύου τότε:
  - Τα δικαιώματα κοινής χρήσης που έχει συσσωρευτικά είναι Full Control
  - Τα συσσωρευτικά του δικαιώματα NTFS είναι Read και Write

Τελικά από αυτά τα δύο θα ισχύσουν τα πιο περιοριστικά δηλαδή, μέσω δικτύου, θα έχει πρόσβαση με δικαιώματα Read και Write.